


RB 135, 934
Presented to the
LIBRARY of the
UNIVERSITY OF TORONTO
by
Department of Mathematics



D. HILBERT

PROFESSEUR A L'UNIVERSITÉ DE GOETTINGUE

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

Ouvrage traduit de l'allemand

PAR

A. LÉVY

PROFESSEUR AU LYCÉE SAINT-LOUIS

et

TH. GOT

ANCIEN INGÉNIEUR DE LA MARINE

AGRÉGÉ DE L'UNIVERSITÉ

Avec une Préface et des Notes de M. G. HUMBERT, Membre de l'Institut et des Notes de M. Th. GOT

PARIS

LIBRAIRIE SCIENTIFIQUE A. HERMANN ET FILS

LIBRAIRES DE S. M. LE ROI DE SUÈDE,

6, RUE DE LA SORBONNE, 6

1913

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

D. HILBERT

PROFESSEUR A L'UNIVERSITÉ DE GOETTINGUE

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

Ouvrage traduit de l'allemand

PAR

A. LÉVY

PROFESSEUR AU LYCÉE SAINT-LOUIS

et

TH. GOT

ANCIEN INGÉNIEUR DE LA MARINE

AGRÉGÉ DE L'UNIVERSITÉ

Avec une Préface et des Notes de M. G. HUMBERT, Membre de l'Institut

et des Notes de M. Th. GOT

PARIS

LIBRAIRIE SCIENTIFIQUE A. HERMANN ET FILS

LIBRAIRES DE S. M. LE ROI DE SUÈDE.

6, RUE DE LA SORBONNE, 6

1913

PRÉFACE

L'ouvrage de M. Hilbert sur la *Théorie des Nombres algébriques* est un de ces Rapports que publie la Société des Mathématiciens allemands et qui fixent l'état de la Science à une époque et dans un domaine. M. Hilbert, sans négliger le point de vue historique, y reprend toute la théorie d'une manière didactique, suivie, complète et personnelle. Il fond, dans un exposé nouveau, tous les résultats acquis; il énonce et enchaîne les propositions avec le plus grand soin, fait ressortir les théorèmes essentiels; enfin, dans les démonstrations, toujours nettes et précises, s'il laisse parfois de côté les points secondaires et faciles, c'est pour mieux mettre en relief le nœud même du raisonnement.

Bien des géomètres, en rédigeant un Mémoire, ont rêvé certainement d'un mode d'exposition où les lignes essentielles seraient marquées en vigueur, et les détails seulement esquissés : l'habitude, la crainte de l'obscurité les ont généralement ramenés dans la route traditionnelle. M. Hilbert a su en sortir. Aussi nul livre n'est-il, pour les mathématiciens, d'une lecture plus attachante : il conduit, sans effort sensible, des parties les plus élémentaires jusqu'aux sommets de cette belle Science des Nombres, déjà si féconde en résultats et si riche encore en promesses. Qui l'a lu, compris et médité possède les méthodes et sait leurs conséquences.

Nous souhaitons que la traduction de MM. Lévy et Got répande en France le goût de théories et de recherches trop délaissées par notre jeune école de mathématiciens.

G. HUMBERT.

AVERTISSEMENT

Mon maître et ami M. Hadamard désirait que l'œuvre de M. Hilbert relative aux nombres algébriques fût connue en France aussi de ceux qui ne possèdent pas assez la langue allemande pour la lire dans le texte original. J'ai été très heureux lorsqu'il m'a prié d'en entreprendre la traduction

Pendant que je faisais ce travail, j'appris qu'un de mes collègues, M. Got, séduit par la beauté des travaux de M. Hilbert, avait déjà traduit son ouvrage. Je me suis empressé de lui demander sa collaboration et je lui suis très reconnaissant de me l'avoir accordée.

L'ouvrage de M. Hilbert s'adresse à des lecteurs auxquels les éléments de la Théorie des nombres soient déjà familiers; il est par suite souvent, surtout dans la première partie, d'une extrême concision et il demande, la plupart du temps, à être lu la plume à la main. Nous n'avions pas qualité pour suppléer par des notes personnelles (1) aux démonstrations manquantes ou très abrégées et nous n'avons pas cru pouvoir mieux faire, pour combler les lacunes les plus importantes, que d'avoir recours aux leçons professées par M. Humbert au Collège de France; nous lui sommes particulièrement reconnaissant de nous avoir autorisé à extraire de ses cahiers plusieurs Notes relatives à des théorèmes fondamentaux de la Théorie générale et des Corps quadratiques.

Nous tenons également à remercier le Comité de direction des *Annales de la Faculté des sciences de Toulouse;* c'est, en effet, en grande partie grâce au concours matériel de cet important Recueil que la publication de notre travail a été assurée.

A. Lévy.

1. M. Got a toutefois pensé être utile, au moins à quelques lecteurs, en reproduisant au bas des pages quelques-uns des calculs tout à fait élémentaires effectués par lui, au cours de sa lecture, pour rétablir parfois des intermédiaires manquants.

PRÉFACE DE L'AUTEUR

La théorie des nombres est une des branches les plus anciennes des sciences mathématiques, et l'esprit humain remarqua de bonne heure quelques propriétés profondes des nombres naturels. Toutefois, ce n'est qu'aux temps modernes qu'elle doit son existence comme science indépendante et systématique.

On vante toujours de cette théorie des nombres la simplicité de ses fondements, la précision de ses notions et la pureté de ses vérités. D'autres branches des connaissances mathématiques ont dû subir des développements plus ou moins longs avant d'atteindre les exigences de la certitude dans les concepts et de la rigueur dans les raisonnements.

Nous ne sommes donc pas surpris de l'enthousiasme qui à toute époque anima ses adeptes. Legendre dit en dépeignant l'amour d'Euler pour la théorie des nombres : « Presque tous les mathématiciens qui s'occupent de la théorie des nombres le font avec passion. » Nous nous rappelons aussi combien notre maître Gauss tenait en honneur la science arithmétique. Dès que, pour la première fois, il eut trouvé à souhait une démonstration d'une remarquable vérité arithmétique, « le charme de ces recherches l'avait tellement ensorcelé que, désormais, il ne put plus les laisser ». Il prisait Fermat, Euler, Lagrange et Legendre « comme des hommes d'une gloire incomparable, car ils ont ouvert les portes du sanctuaire de cette science divine et ont montré ce qu'il contient de richesses ».

C'est une particularité de la théorie des nombres que la difficulté de la démonstration de certaines vérités simples découvertes facilement par voie

d'induction. « Et précisément ce qui donne à l'Arithmétique supérieure », dit Gauss, « ce charme magique qui en a fait la science préférée des géomètres, c'est de ne pas douter de ses richesses inépuisables qui surpassent celles de toutes les autres parties des mathématiques ».

On connaît la préférence de Lejeune-Dirichlet pour l'Arithmétique, l'activité de Kummer fut consacrée surtout à la Théorie des nombres, et Kronecker exprima les sentiments de son cours de mathématicien en ces termes : « Dieu fit le nombre entier, le reste est œuvre de l'homme. »

Si l'on tient compte de la rareté de ses pétitions de principe, la théorie des nombres est certainement la branche de la connaissance mathématique dont les vérités sont les plus faciles à saisir.

Mais pour comprendre et se rendre maître des concepts arithmétiques, l'esprit doit posséder une grande faculté d'abstraction, — c'est là un reproche que l'on fait quelquefois à l'Arithmétique. — Je suis d'avis que les autres branches des mathématiques exigent une faculté d'abstraction au moins égale, en admettant que dans ces domaines aussi on apporte la même rigueur et la même perfection dans l'examen des notions fondamentales.

En ce qui concerne le rôle de la théorie des nombres dans l'ensemble des sciences mathématiques, Gauss, dans sa Préface des *Disquisitiones arithmeticæ*, considère encore la théorie des nombres comme une théorie des nombres naturels en excluant expressément les nombres imaginaires.

D'après cela, il ne considère pas que la théorie de la division du cercle (Kreisteilung) appartient à la théorie des nombres; mais il ajoute « que ces principes peuvent être tirés tout entiers et uniquement de l'Arithmétique supérieure ». A côté de Gauss, Jacobi et Lejeune-Dirichlet expriment maintes fois et avec force leur surprise à propos des rapports étroits entre les questions concernant les nombres et certains problèmes algébriques, en particulier les problèmes de la division du cercle. La raison intime de ces rapports est parfaitement découverte aujourd'hui. La théorie des nombres algébriques et la théorie des équations de Galois ont leurs racines communes dans la Théorie des corps algébriques, et cette théorie du corps de nombres est devenue la partie la plus importante de la théorie moderne des nombres.

Le mérite d'avoir apporté le premier germe de la théorie du corps de nombres appartient encore à Gauss. Gauss reconnut que la source naturelle pour arriver aux lois des restes biquadratiques était « l'extension du champ de l'arithmétique », comme il dit, cette extension s'obtenant par l'intro-

duction des nombres entiers imaginaires de la forme $a+bi$: il posa et résolut le problème d'étendre à ces nombres imaginaires toutes les lois de la divisibilité et des propriétés des congruences des nombres ordinaires. Plus tard, Dedekind et Kronecker, en développant et généralisant cette pensée et en se basant sur les idées de Kummer ayant une portée plus grande, arrivèrent à établir notre théorie actuelle du corps de nombres algébriques.

La théorie des nombres n'est pas en rapport seulement avec l'algèbre, mais elle est aussi étroitement liée à la théorie des fonctions. Nous rappellerons les analogies nombreuses et merveilleuses entre certains faits de la théorie des nombres algébriques et la théorie des fonctions algébriques d'une variable; de plus, les recherches profondes de Riemann, qui déduit la réponse à la question de la densité des nombres premiers de la connaissance des zéros d'une certaine fonction analytique. La transcendance des nombres e et π est aussi une propriété arithmétique d'une fonction analytique, la fonction exponentielle.

Enfin, la méthode si importante et à si grande portée imaginée par Lejeune-Dirichlet, pour déterminer le nombre des classes d'un corps de nombres, repose sur des bases analytiques.

Les fonctions périodiques et certaines fonctions à transformations linéaires touchent plus profondément par leur nature intime au nombre : ainsi la fonction exponentielle $e^{2i\pi z}$ peut être considérée, comme l'invariant de l'ensemble des nombres entiers rationnels, comme solution fondamentale de l'équation fonctionnelle $f(z+1)=f(z)$.

De plus, Jacobi avait déjà ressenti le rapport étroit entre la théorie des fonctions elliptiques et la théorie des irrationnalités quadratiques; il va même jusqu'à supposer que l'idée de Gauss, citée plus haut, d'introduire les nombres entiers imaginaires de la forme $a+bi$ ne lui est pas venue rien que par des considérations arithmétiques, mais aussi par des recherches simultanées sur les fonctions de la lemniscate et de leur multiplication complexe. Les fonctions elliptiques, pour certaines valeurs de leurs périodes, et la fonction modulaire elliptique sont toujours l'invariant d'un nombre entier d'un certain corps quadratique imaginaire. Ces fonctions, désignées sous le nom d'invariant, permettent de résoudre certains problèmes difficiles et profondément cachés de la théorie des corps algébriques correspondants, et, réciproquement, la théorie des fonctions elliptiques doit à ces conceptions arithmétiques et à leur application un nouvel essor.

Nous voyons comment l'arithmétique, « reine » de la science mathématique, conquiert de vastes domaines de l'algèbre et de la théorie des fonctions, et comment elle leur enlève le rôle de guide. Que cela ne se soit pas produit plus tôt et dans une mesure plus vaste, cela tient, il me semble, à ce que la théorie des nombres n'a atteint sa maturité qu'à une époque récente. Même Gauss se plaint des efforts démesurés que lui a coûté la détermination du signe d'un radical dans la théorie des nombres; « bien d'autres choses ne l'ont pas retenu autant de jours que cette question l'a retenu d'années »; puis tout à coup, « comme tombe la foudre, l'énigme est résolue ». La construction de la théorie du corps quadratique a apporté de nos jours un développement sûr et continu, au lieu des progrès par bonds qui caractérisaient la science dans son jeune âge.

Il faut ajouter enfin, si je ne me trompe, que, d'une façon générale, le développement des mathématiques pures dans les temps modernes s'opère principalement sous le signe du nombre : les définitions dues à Dedekind et à Weierstrass des notions fondamentales de l'arithmétique, et les ensembles numériques de Cantor ont établi ce principe, qu'un fait de la théorie des fonctions ne doit être considéré comme démontré que si, en dernière instance, il se ramène à des rapports entre des nombres entiers rationnels.

La géométrie s'est arithmétisée par les recherches modernes concernant la géométrie non-euclidienne; ces recherches tentent d'établir la géométrie avec une logique sévère et s'occupent d'introduire le nombre en géométrie sans prêter à la moindre objection.

Le but de ce rapport est d'exposer un développement logique des faits de la théorie des nombres et leurs démonstrations d'après différents points de vue, et de coopérer ainsi à faire avancer l'heure à laquelle les conquêtes de nos grands classiques de la théorie des nombres seront devenues la propriété commune de tous les mathématiciens.

J'ai évité complètement les citations historiques et les attributions de priorité. Disposant d'un espace assez restreint, je me suis efforcé de rechercher partout les sources les plus riches, et toutes les fois que j'ai dû choisir, j'ai donné la préférence aux moyens qui me semblaient les plus profonds et ayant la plus grande portée. On ne juge pas en soi-même quelle est, parmi plusieurs démonstrations, la plus simple et la plus naturelle; il faut d'abord savoir si les principes invoqués sont susceptibles d'une généralisation et s'ils peuvent nous conduire à d'autres recherches.

La première partie de ce rapport traite de la théorie générale du corps algébrique ; cette théorie nous apparaît comme un édifice considérable assis sur trois piliers principaux : le théorème de la décomposition unique des nombres en idéaux premiers, le théorème relatif à l'existence des unités et enfin la détermination transcendante du nombre des classes. La deuxième partie renferme la théorie des corps de Galois, qui à son tour contient la théorie générale. La troisième partie est consacrée à l'exemple classique du corps quadratique. La quatrième partie traite le corps du cercle. La cinquième partie développe la théorie du corps que Kummer a pris comme base dans ses recherches sur les réciprocités d'ordre supérieur. C'est pourquoi je l'ai appelé corps de Kummer. La théorie de ce corps de Kummer est le sommet le plus élevé qu'ait atteint la science arithmétique actuelle. De ce sommet, on aperçoit bien tout le domaine acquis par la science, car presque toute idée ou toute notion de la théorie des corps, au moins prise dans un sens particulier, trouve son application dans la démonstration des lois supérieures de réciprocité. J'ai essayé d'éviter le grand appareil de calculs de Kummer, pour réaliser aussi ici l'idée fondamentale de Riemann qu'il faut triompher des démonstrations non par le calcul, mais par la pensée.

Les théories de la troisième, de la quatrième et de la cinquième partie sont toutes des théories de corps abéliens particuliers ou de corps abéliens relatifs. Un autre exemple d'une pareille théorie serait la multiplication complexe des fonctions elliptiques, en les considérant comme une théorie des corps qui sont des corps abéliens relatifs par rapport à un corps imaginaire quadratique donné. J'ai dû renoncer à faire entrer ces recherches sur la multiplication complexe dans ce rapport, car les faits de cette théorie n'ont pas encore été l'objet de travaux assez simples et assez complets pour permettre une exposition satisfaisante.

La théorie des corps de nombres est un monument d'une admirable beauté et d'une incomparable harmonie ; la plus belle partie de ce monument me semble être la théorie des corps abéliens et des corps abéliens relatifs. Kummer et Kronecker nous l'ont révélée, l'un par ses travaux sur les lois supérieures de réciprocité, l'autre par ses recherches sur la multiplication complexe des fonctions elliptiques.

Les vues profondes que nous donne l'œuvre de ces mathématiciens dans cette théorie, nous montrent aussi que dans ce domaine de la science une

foule de trésors les plus précieux demeurent encore cachés; attraits d'une belle récompense qui doivent tenter le chercheur qui connaît la valeur de pareils trésors et qui pratique avec amour l'art de les découvrir.

Les cinq parties de ce rapport sont subdivisées en chapitres et en paragraphes; dans ces paragraphes, les énoncés des théorèmes précèdent les lemmes et sont suivis des démonstrations. Je considère le lecteur comme un voyageur : les lemmes sont des haltes, les théorèmes sont les stations plus importantes désignées à l'avance, de façon à ne pas fatiguer la faculté d'assimilation. J'ai signalé par une impression spéciale les théorèmes qui sont en eux-mêmes un but principal à cause de leur importance même, et aussi ceux qui peuvent être pris pour point de départ d'incursions dans un pays nouveau et non encore découvert.

Ce sont les théorèmes 7 (§ 5), 31 (§ 10), 40 (§ 16), 44 (§ 18), 45 (§ 18), 47 (§ 19), 56 (§ 26), 82 (§ 49), 94 (§ 58), 100 (§ 67), 101 (§ 69), 131 (§ 100), 143 (§ 119), 144 (§ 120), 150 (§ 130), 158 (§ 147), 159 (§ 148), 161 (§ 154), 164 (§ 163), 166 (§ 164), 167 (§ 165).

Le livre est précédé d'une table des matières et d'une indication des auteurs cités. Tout à la fin, j'ai placé une table des concepts de l'ouvrage.

Mon ami Hermann Minkowski a corrigé avec soin les épreuves et a lu la plus grande partie du manuscrit. J'ai fait sur sa prière bien des améliorations formelles et matérielles; je lui exprime ici toute ma reconnaissance pour l'aide qu'il m'a prêtée.

Je remercie aussi ma femme qui a écrit tout le manuscrit et a fait les tables.

J'exprime également ma reconnaissance au Comité de rédaction de la *Deutsche Mathematiker Vereinigung*, en particulier à M. Gutzmer, qui a lu les épreuves, et à la maison d'édition Georges Reimer, qui m'a prêté la plus grande complaisance pour la composition et l'impression.

D. HILBERT.

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

MÉMOIRE de M. DAVID HILBERT,

Professeur à l'Université de Gœttingen.

PUBLIÉ PAR LA SOCIÉTÉ

DEUTSCHE MATHEMATIKER VEREINIGUNG, en 1897.

TRADUIT PAR M. A. LEVY,

Professeur au Lycée Voltaire.

Toutes les fois que M. Hilbert cite un auteur, le nom de cet auteur est accompagné d'un chiffre ; ce chiffre, en se reportant à la table des renvois, indique l'ouvrage de l'auteur se rapportant à la question.

Nous mettrons cette table en tête des articles qui vont paraître.

TABLE DES OUVRAGES CITÉS DANS LE TEXTE.

N.-H. Abel.

1. *Extraits de quelques lettres à Holmboe.* Œuvres, 2e vol., p. 254.

F. Arndt.

1. *Bemerkungen über die Verwandlung der irrationalen Quadratwurzel in einen Kettenbruch.* Journ. für Math., t. XXXI, 1846.

P. Bachmann.

1. *Zur Theorie der complexen Zahlen.* Journ. für Math., t. LXVII, 1867.
2. *Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie.* Leipzig, 1872.
3. *Ergänzung einer Untersuchung von Dirichlet.* Math. Ann., t. XVI, 1880.

H. Berkenbusch.

1. *Ueber die aus den 8 ten Wurzeln der Einheit entspringenden Zahlen.* Inauguraldissertation. Marburg, 1891.

A.-L. Cauchy.

1. *Mémoire sur la théorie des nombres.* Comptes rendus, 1840.
2. *Mémoire sur diverses propositions relatives à la théorie des nombres* (trois Notes). Comptes rendus, 1847.

A. Cayley.

1. *Table des formes quadratiques binaires pour les déterminants négatifs depuis* D = — 1 *jusqu'à* D = — 100, *pour les déterminants positifs non carrés depuis* D = 2 *jusqu'à* D = 99 *et pour les treize déterminants négatifs irréguliers qui se trouvent dans le premier millier.* Œuvres, t. V, p. 141, 1862.

R. Dedekind.

1. *Vorlesungen über Zahlentheorie von P. G. Lejeune-Dirichlet.* Auflage II bis IV. Braunschweig, 1871-1894. Supplément XI et Supplément VII.
2. *Sur la théorie des nombres entiers algébriques.* Paris, 1877. Bull. des sciences math. et astron., t. I, p. 2, et t. XI, p. 1.
3. *Ueber die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers.* Braunschweig, 1877.
4. *Ueber den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen.* Abh. der K. Ges. der Wiss. zu Göttingen, 1878.
5. *Sur la théorie des nombres complexes idéaux.* Comptes rendus, t. XC, 1880.
6. *Ueber die Discriminanten endlicher Körper.* Abh. der K. Ges. der Wiss. zu Göttingen, 1882.
7. *Ueber einen arithmetischen Satz von Gauss.* Mitteilungen der deutschen math. Ges zu Prag 1892, und : *Ueber die Begründung der Idealtheorie.* Nachr. d. K. Ges. der Wiss. zu Göttingen, 1895.
8. *Zur Theorie der Ideale.* Nachr. der K. Ges. der Wiss. zu Göttingen, 1894.
9. *Ueber eine Erweiterung des Symbols* ($\mathfrak{a}$, $\mathfrak{b}$) *in der Theorie der Moduln.* Nachr. der K. Ges. der Wiss. zu Göttingen, 1895.

G. Lejeune Dirichlet.

1. *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré.* Œuvres, t. I, p. 1, 1825.
2. *Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré.* Œuvres, t. I, p. 21, 1825, 1828.
3. *Démonstration du théorème de Fermat pour le cas des quatorzièmes puissances.* Œuvres, t. I, p. 189, 1832.
4. *Einige neue Sätze über unbestimmte Gleichungen.* Œuvres, t. I, p. 219, 1834.
5. *Démonstration d'un théorème sur la progression arithmétique.* Œuvres, t. I, p. 307, 1837.
6. *Démonstration du théorème que toute progression arithmétique dont le premier terme et la raison sont des nombres entiers sans diviseur commun contient un nombre infini de nombres premiers.* Œuvres, t. I, p. 313, 1837.
7. *Sur la manière de résoudre l'équation* $t^2 - pu^2 = 1$ *au moyen des fonctions circulaires.* Œuvres, t. I, p. 343.
8. *Sur l'usage des séries infinies dans la théorie des nombres.* Œuvres, t. I, p. 357, 1838.

9. *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres.* Œuvres, t. I, p. 411, 1839-1840.

10. *Untersuchungen über die Theorie der complexen Zahlen.* Œuvres, t. I, p. 503, 1841.

11. *Untersuchungen über die Theorie der complexen Zahlen.* Œuvres, t. I, p. 509, 1841.

12. *Recherches sur les formes quadratiques à coefficients et à indéterminées complexes.* Œuvres, t. I, p. 533, 1842.

13. *Sur la théorie des nombres.* Œuvres, t. I, p. 619, 1840.

14. *Einige Resultate von Untersuchungen über eine Klasse homogener Functionen des dritten und der höheren Grade.* Œuvres, t. I, p. 625, 1841.

15. *Sur un théorème relatif aux séries.* Journ. für Math., t. LIII, 1857.

16. *Verallgemeinerung eines Satzes aus der Lehre von den Kettenbrüchen nebst einigen Anwendungen auf die Theorie der Zahlen.* Œuvres, t. I, p. 653, 1842, und : *Zur Theorie der complexen Einheiten.* Œuvres, t. I, p. 639, 1846.

G. Eisenstein.

1. *Ueber eine neue Gattung zahlentheoretischer Functionen.* Bericht der K. Akad. der Wiss. zu Berlin, 1850.

2. *Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen.* Bericht. der K. Akad. der Wiss. zu Berlin, 1880.

3. *Ueber die Anzahl der quadratischen Formen, welche in der Theorie der complexen Zahlen zu einer reellen Determinante gehören.* Journal für Math., t. XXVII, 1844.

4. *Beiträge zur Kreisteilung.* Journal für Math., t. XXVII, 1844.

5. *Beweis des Reciprocitätsgesetzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten Zahlen.* Journal für Math., t. XXVII, 1844.

6. *Ueber die Anzahl der quadratischen Formen in den verschiedenen complexen Theorien.* Journal für Math., t. XXVII, 1844.

7. *Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Kriterien des cubischen Charakters der Zahl 3 und ihrer Teiler.* Journal für Math., t. XXVIII, 1844.

8. *Loi de réciprocité. Nouvelle démonstration du théorème fondamental sur les résidus quadratiques dans la théorie des nombres complexes. Démonstration du théorème fondamental sur les résidus biquadratiques qui comprend comme cas particulier le théorème fondamental.* Journal für Math., t. XXVIII, 1844.

9. *Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste.* Journal für Math., t. XXVIII, 1844.

10. *Untersuchungen über die Formen dritten Grades mit drei Variabeln welche der Kreisteilung ihre Entstehung verdanken.* Journal für Math., t. XXVIII et XXIX, 1844, 1845.

11. *Zur Theorie der quadratischen Zerfällung der Primzahlen $8n+3$, $7n+2$ et $7n+4$.* Journal für Math., t. XXXVII, 1848.

12. *Ueber ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungsgesätze.* Journal für Math., t. XXXIX, 1850.

G. Frobenius.

1. *Ueber Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe.* Berichte der K. Akad. Wiss. zu Berlin, 1896.

L. Fuchs.

1. *Ueber die Perioden, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebilded sind, wenn n eine zusammengesetzte Zahl ist.* Journal für Math., t. LXI, 1862.

2. *Ueber die aus Einheitswurzeln gebildeten complexen Zahlen von periodischem Verhalten, insbesondere die Bestimmung der Klassenanzahl derselben.* Journal für Math., t. LXV, 1864.

C. F. Gauss.

1. *Disquisitiones arithmeticae*, 1801. Œuvres, t. I.
2. *Summatio quarundam serierum singularium*. Œuvres, t. II, p. 11.
3. *Theoria residuorum biquadraticorum, commentatio prima et secunda*. Œuvres, t. II, pp. 65 et 93.

J. A. Gmeiner.

1. *Die Ergänzungssätze zum bicubischen Reciprocitätsgesetze*. Ber. der K. Akad. der Wiss. zu Wien, 1892.
2. *Das allgemeine bicubische Reciprocitätsgesetz*. Ber. der K. Akad. der Wiss. zu Wien, 1892.
3. *Die bicubische Reciprocität zwischen einer reellen und einer zweigliedrigen regulären Zahl*. Monatshefte für Math. und Phys., t. III, 1892.

K. Hensel.

1. *Arithmetische Untersuchungen über Discriminanten und ihre ausserwesentlichen Teiler*. Inaugural-Dissert. Berlin, 1884.
2. *Darstellung der Zahlen eines Gattungsbereiches für einen beliebigen Primdivisor*. Journal für Math., t. CI et CIII, 1887, 1888.
3. *Ueber Gattungen, welche durch Composition aus zwei anderen Gattungen entstehen*. Journal für Math., t. CV, 1889.
4. *Untersuchung der Fundamentalgleichungen einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Teiler ihrer Discriminante*. Journal für Matth., t. CXIII, 1894.
5. *Arithmetische Untersuchungen ueber die gemeinsamen ausserwesentlichen Discriminantenteiler einen Gattung*. Journal für Matth., t. CXIII, 1894.

Ch. Hermite.

1. *Sur la théorie des formes quadratiques ternaires indéfinies*. Journal für Math., t. XLVII, 1854.
2. *Extrait d'une lettre de M. Ch. Hermite à H. Borchardt sur le nombre limité d'irrationalités auxquelles se réduisent les racines des équations à coefficients entiers complexes d'un degré et d'un discriminant donnés*. Journal für Math., t. LIII, 1857.

D. Hilbert.

1. *Zwei neue Beweise für die Zerlegbarkeit der Zahlen eines Körpers in Primideale*. Jahresber. der Deutschen Mathematiker-Vereinigung, t. III, 1893.
2. *Ueber die Zerlegung der Ideale eines Körpers in Primideale*. Math. Ann., t. XLIV, 1894.
3. *Grundzüge einer theorie des Galois'schen Zahlkörpers*. Nachr. der K. Ges. der Wiss. zu Göttingen, 1894.
4. *Ueber den Dirichlet'schen biquadratischen Zahlkörper*. Math. Ann., t. XLV, 1894.
5. *Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper*. Nachr. der K. Ges. der Wiss. zu Göttingen, 1896.

A. Hurwitz.

1. *Ueber die Theorie der Ideale*. Nachr. der K. Ges. der Wiss. zu Göttingen, 1894.
2. *Ueber einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen*. Nachr. der K. Ges. der Wiss. zu Göttingen, 1895.

3. *Zur Theorie der algebraischen Zahlen.* Nachr. der K. Ges. der Wiss. zu Gottingen, 1895.
4. *Die unimodularen Substitutionen in einem algebraischen Zahlenkörper.* Nachr. der K. Ges. der Wiss. zu Göttingen, 1895.

C. G. J. Jacobi.

1. *De residuis cubicis commentatio numerosa.* Œuvres, t. VI.
2. *Observatio arithmetica de numero classium divisorum quadraticorum formae $y^2 + Az^2$ designante A numerum primum formae $4n + 3$.* Œuvres, t. VI, p. 240, 1832.
3. *Ueber die Kreisteilung und ihre Anwendung auf die Zahlentheorie.* Œuvres, t. VI, p. 254, 1837.
4. *Ueber die complexen Primzahlen, welche in der Theorie der Reste der 5ten 8ten und 12ten Potenzen zu betrachten sind.* Œuvres, t. VI, p. 275, 1839.

L. Kronecker.

1. *De unitatibus complexis. Dissertatio inauguralis.* Berolini, 1845. Œuvres, t. I, p. 5, 1845.
2. *Ueber die algebraisch auflösbaren Gleichungen.* Ber. der K. Akad. der Wiss. zu Berlin, 1853.
3. *Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$.* Œuvres, t. I, p. 75, 1854.
4. *Sur une formule de Gauss.* Journal de Math., 1856.
5. *Démonstration d'un théorème de M. Kummer.* Œuvres, t. I, p. 93, 1856.
6. *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten.* Œuvres, t. I, p. 103, 1857.
7. *Ueber complexe Einheiten.* Œuvres, t. I, p. 109, 1857.
8. *Ueber cubische Gleichungen mit rationalen Coefficienten.* Œuvres, t. I, p. 119, 1859.
9. *Ueber die Klassenanzahl der aus Wurzeln der Einheit gebildeten complexen Zahlen.* Œuvres, t. I, p. 123, 1863.
10. *Ueber den Gebrauch der Dirichlet'schen Methoden in der Theorie der quadratischen Formen.* Ber. der K. Akad. der Wiss. zu Berlin, 1864.
11. *Auseinandersetzung einiger Eigenschaften der Klassenanzahl idealer complexer Zahlen.* Œuvres, t. I, p. 271, 1870.
12. *Bemerkungen über Reuschle's Tafeln complexer Primzahlen.* Ber. der K. Akad. der Wiss. zu Berlin, 1875.
13. *Ueber Abel'sche Gleichungen.* Ber. der K. Akad. der Wiss. zu Berlin, 1877.
14. *Ueber die Irreductibilität von Gleichungen.* Ber. der K. Akad. der Wiss. zu Berlin, 1880.
15. *Ueber die Potenzreste gewisser complexer Zahlen.* Ber. der K. Akad. der Wiss. zu Berlin, 1880.
16. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen.* Journal für Math., t. XCII, 1882.
17. *Zur Theorie der Abel'schen Gleichungen. Bemerkungen zum vorangehenden Aufsatz des Herrn Schwering.* Journ. für Math., t. XCIII, 1882.
18. *Sur les unités complexes* (trois Notes). Comptes rendus, t. XCVI, 1883. — Comparez avec J. Molk : *Sur les unités complexes.* Bull. des sc. math. et astr., 1883.
19. *Zur Theorie der Formen höherer Stufen.* Ber. der K. Akad. der Wiss. zu Berlin, 1883.
20. *Additions au mémoire sur les unités complexes.* Comptes rendus, t. XCIX, 1884.
21. *Ein Satz über Discriminanten-Formen.* Journal für Math., t. C, 1886.

E. Kummer.

1. *De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda.* Journal für Math., t. XVII, 1837.
2. *Eine Aufgabe, betreffend die Theorie der cubischeu Reste.* Journal für Math., t. XXIII, 1842.

3. *Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreisteilung entstehen*. Journal für Math., t. XXX, 1846.

4. *De residuis cubicis disquisitiones nonnullae analyticae*. Journal für Math., t. XXXII, 1846.

5. *Zur Theorie der complexen Zahlen*. Journal für Math., t. XXXV, 1847.

6. *Ueber die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in Primfactoren*. Journal für Math., t. XXXV, 1847.

7. *Bestimmung der Anzahl nicht aequivalenter Klassen für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben*. Journal für Math., t. XL, 1850.

8. *Zwei besondere Untersuchungen über die Klassenanzahl und über die Einheiten der aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen*. Journal für Math., t. XL, 1850.

9. *Allgemeiner Beweis des Fermat'schen Satzes, dass die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen lösbar ist, für alle diejenigen Potenz-Exponenten λ, welche ungerade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoulli'schen Zahlen als Factoren nicht vorkommen*. Journal für Math., t. XL, 1850.

10. *Ueber allgemeine Reciprocitätsgesetze für beliebig hohe Potenzreste*. Ber. der K. Akad. der Wiss. zu Berlin, 1850.

11. *Mémoire sur les nombres complexes composés de racines de l'unité et des nombres entiers*. Journal de math., t. XVI, 1851.

12. *Ueber die Ergänzungsätze zu den allgemeinen Reciprocitätsgesetzen*. Journal für Math., t. XLIV, 1851.

13. *Ueber die Irregularität der Determinanten*. Ber. der K. Akad. der Wiss. zu Berlin, 1853.

14. *Ueber eine besondere Art aus complexen Einheiten gebildeter Ausdrücke*. Journal für Math., t. L, 1854.

15. *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist*. Abh. der K. Akad. der Wiss. zu Berlin, 1856.

16. *Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen für den Fall, dass die Klassenanzahl durch λ teilbar ist nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermat'schen Lehrsatzes*. Abh. der K. Akad. der Wiss. zu Berlin, 1857.

17. *Ueber die den Gauss'chen Perioden der Kreisteilung entsprechenden Congruenzwurzeln*. Journal für Math., t. LIII, 1856.

18. *Ueber die allgemeinen Reciprocitätsgesetze der Potenzreste*. Ber. der K. Acad. der Wiss., zu Berlin, 1858.

19. *Ueber die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*. Journal für Matth., t. LVI, 1858.

20. *Ueber die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*. Abh. der K. Akad. der Wiss. zu Berlin, 1859.

21. *Zwei neue Beweise der allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist*. Abh. der K. Akad. der Wiss. zu Berlin, 1861. Reproduit dans le *Journal für Math.*, t. C.

22. *Ueber die Klassenanzahl der aus n^{ten} Einheitswurzeln gebildeten idealen complexen Zahlen*. Ber. der K. Akad. der Wiss. zu Berlin, 1861.

23. *Ueber die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen complexen Zahlen*. Ber. der K. Akad. der Wiss. zu Berlin, 1863.

24. *Ueber die einfachste Darstellung der aus Einheitswurzeln gebildeten complexen Zahlen, welche durch Multiplication mit Einheiten bewirkt werden kann*. Ber. der K. Akad. der Wiss. zu Berlin, 1870.

25. *Ueber eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen und über den zweiten Factor der Klassenanzahl.* Ber. der K. Akad. der Wiss. zu Berlin, 1870.

26. *Ueber diejenigen Primzahlen λ, für welche die Klassenanzahl der aus λ^{ten} Einheitswurzeln gebildeten complexen Zahlen durch λ teilbar ist.* Ber. der K. Akad. der Wiss. zu Berlin, 1874.

J.-L. Lagrange.

1. *Sur la solution des problèmes indéterminés du second degré.* Œuvres, t. II, p. 375.

G. Lamé.

1. *Mémoire d'analyse indéterminée démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers.* Journal de Math., 1840.

2. *Mémoire sur la résolution en nombres complexes de l'équation* $A^5 + B^5 + C^5 = 0$. Journal de Math., 1847.

3. *Mémoire sur la résolution en nombres complexes de l'équation* $A^n + B^n + C^n = 0$. Journal de Math., 1847.

V.-A. Lebesgue.

1. *Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers.* Journal de Math., 1840.

2. *Additions à la note sur l'équation $x^7 + y^7 + z^7 = 0$.* Journal de Math., 1840.

3. *Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$.* Journal de Math., 1843.

A. Legendre.

1. *Essai sur la théorie des nombres*, 1798.

F. Mertens.

1. *Ueber einen algebraischen Satz.* Ber. der K. Akad. der Wiss. zu Wien, 1892.

C. Minnigerode.

1. *Ueber die Verteilung der quadratischen Formen mit complexen Coefficienten und Veränderlichen in Geschlechter.* Nachr. der K. Ges. der Wiss. zu Göttingen, 1873.

H. Minkowsky.

1. *Ueber die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen.* Journal für Math., t. CVII, 1891.

2. *Théorèmes arithmétiques. Extrait d'une lettre à M. Hermite.* Comptes rendus, t. XII, 1891.

3. *Geometrie der Zahlen.* Leipzig, 1896.

4. *Généralisation de la théorie des fractions continues.* Ann. de l'École normale, 1896.

C.-G. Reuschle.

1. *Tafeln complexer Primzahlen, welche aus Wurzeln der Einheit gebildet sind.* Berlin, 1875.

E. Schering.

1. *Zahlentheoretische Bemerkung. Auszug aus einem Brief an Herrn Kronecker.* Journal für Math., t. C.
2. *Die Fundamentalklassen der zusammengesetzten Formen.* Abh. der K. Ges. der Wiss. zu Göttingen, 1869.

K. Schwering.

1. *Zur Theorie der arithmetischen Functionen, welche von Jacobi $\psi(a)$ genannt werden.* Journal für Math., t. XCIII, 1882.
2. *Untersuchung über die fünften Potenzreste und die aus fünften Einheitswurzeln gebildeten ganzen Zahlen.* Zeitschrift für Math. und Physik, t. XXVII, 1882.
3. *Ueber gewisse trinomische complexe Zahlen.* Acta Math., t. X, 1887.
4. *Une propriété du nombre premier 107.* Acta Math., t. XI, 1887.

J.-A. Serret.

1. *Traité d'algèbre supérieure.*

H. Smith.

1. *Report on the theory of numbers.* Œuvres.

L. Stickelberger.

1. *Ueber eine Verallgemeinerung der Kreisteilung.* Math. Ann., t. XXXVII, 1890.

F. Tano.

1. *Sur quelques théorèmes de Dirichlet.* Journal für Math., t. CV.

H. Weber.

1. *Theorie der Abel'schen Zahlkörper.* Acta Math., t. VIII et IX, 1886 et 1887.
2. *Ueber Abel'sche Zahlkörper dritten und vierten Grades.* Sitzungsber. der Ges. zur Förderung der Naturw. zu Marburg, 1892.
3. *Zahlentheoretische Untersuchungen aus dem Gebiete der elliptischen Functionen.* Nachr. der K. Ges. der Wiss. zu Göttingen, 1893. (Drei Mitteilungen.)
4. *Lehrbuch der Algebra.* Braunschweig, 1896.

P. Wolfskehl.

1. *Beweis, dass der zweite Factor der Klassenanzahl für die aus den elften und dreizehnten Einheitswurzeln gebildeten Zahlen gleich eins ist.* Journal für Math., t. XCIX, 1885.

PREMIÈRE PARTIE.

THÉORIE GÉNÉRALE DU CORPS ALGÉBRIQUE.

CHAPITRE PREMIER.

Le nombre algébrique et le corps algébrique.

§ 1. — LE CORPS ALGÉBRIQUE ET LES CORPS ALGÉBRIQUES CONJUGUÉS.

Un nombre α est dit un *nombre algébrique* s'il satisfait à une équation de degré m de la forme

$$\alpha^m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \ldots + a_m = 0$$

où $a_1, a_2, \ldots, a_m$ sont des nombres rationnels.

Soient $\alpha, \beta, \ldots, \varkappa$ des nombres algébriques quelconques en nombre fini, toutes les fonctions rationnelles à coefficients entiers de $\alpha, \beta, \ldots, \varkappa$ forment un système fermé de nombres algébriques que l'on nomme *Corps de nombres, corps* au domaine de rationalité [Dedekind[1, 2], Kronecker[16]]. Comme en particulier la somme, la différence et le quotient de deux nombres d'un domaine de rationalité est encore un nombre de ce domaine, cette notion de domaine est un invariant relativement aux quatre opérations élémentaires : addition, soustraction, multiplication, division.

THÉORÈME 1. — Dans tout corps k il existe un nombre θ tel que tous les autres nombres du corps sont des fonctions rationnelles entières de θ à coefficients rationnels.

Le degré m de l'équation de plus bas degré à coefficients rationnels satisfaite par θ s'appelle le *degré du corps k*. Le nombre θ est dit le nombre qui *détermine le corps k*.

L'équation de degré m est irréductible dans le domaine de rationalité des nombres rationnels.

Réciproquement, chaque racine d'une pareille équation irréductible détermine un corps de degré m.

Si $\theta', \theta'', \ldots, \theta^{(m-1)}$ sont les $m - 1$ autres racines de l'équation, les corps $k', k'', \ldots, k^{(m-1)}$ déterminés respectivement par $\theta', \theta'', \ldots, \theta^{(m-1)}$ sont dits *les corps conjugués du corps k*.

Soit α un nombre quelconque du corps k et soit

$$\alpha = c_1 + c_2\theta + \ldots + c_m\theta^{m-1},$$

où $c_1, c_2, \ldots, c_m$ sont des nombres rationnels, les nombres

$$\alpha' = c_1 + c_2\theta' + \ldots + c_m\theta'^{m-1},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\alpha^{(m-1)} = c_1 + c_2\theta^{(m-1)} + \ldots + c_m(\theta^{(m-1)})^{m-1}$$

sont dits les nombres *conjugués de* α ou encore les nombres issus de α par les substitutions

$$t' = (\theta : \theta'), \ldots, t^{(m-1)} = (\theta : \theta^{(m-1)}).$$

§ 2. — Le nombre algébrique entier.

Le nombre α est dit un *nombre entier algébrique* ou tout simplement un *nombre entier* s'il satisfait à une équation de la forme

$$\alpha_m + a_1\alpha^{m-1} + a_2\alpha^{m-2} + \ldots + a_m = 0,$$

où $a_1, a_2, \ldots, a_m$ sont des nombres rationnels et entiers.

Théorème 2. — Toute fonction entière F à coefficients entiers d'un nombre quelconque d'entiers $\alpha, \beta, \ldots, \varkappa$ est encore un nombre entier.

Démonstration. — Désignons par $\alpha', \alpha'', \ldots, \beta', \beta'', \ldots, \varkappa', \varkappa'', \ldots$ les nombres conjugués à $\alpha, \beta, \ldots, \varkappa$ et formons toutes les expressions de la forme

$$F(\alpha, \beta, \ldots, \quad F(\alpha', \beta, \ldots, \varkappa), \quad F(\alpha, \beta', \ldots, \varkappa), \quad F(\alpha, \beta, \ldots, \varkappa'), \quad F(\alpha'\beta', \ldots, \varkappa), \quad \ldots$$

le théorème connu sur les fonctions symétriques nous apprend que l'équation à laquelle satisfont ces expressions n'a que des coefficients entiers et que le coefficient de la plus haute puissance $= 1$.

En particulier, la somme, la différence et le produit de deux nombres entiers est un nombre entier. Le concept « entier » est un invariant pour les trois opérations : addition, soustraction, multiplication.

Le nombre entier γ est dit *divisible* par le nombre entier α s'il existe un nombre entier γ tel que $\alpha = \beta\gamma$.

Théorème 3. — Les racines d'une équation quelconque de degré r de la forme

$$\alpha^r + a_1\alpha^{r-1} + a_2\alpha^{r-2} + \ldots + a_r = 0$$

sont toujours des nombres entiers, dès que les coefficients $a_1, a_2, \ldots, a_r$ sont des nombres algébriques entiers.

Théorème 4. — Lorsqu'un nombre entier algébrique est rationnel, il est un nombre entier rationnel.

Démonstration. — Si on avait $\alpha = \frac{a}{b}$, a et b étant rationnels entiers et premiers entre eux et $b > 1$, et si α satisfait à une équation dont les coefficients $a_1, \ldots, a_m$ sont des entiers rationnels, on aurait, en multipliant par b^{m-1},

$$\frac{a^m}{b} = -a_1 a^{m-1} - a_2 b a^{m-2} - \ldots - a_m b^{m-1} = A$$

où A est un nombre entier rationnel, ce qui est impossible. [Dedekind [1], Kronecker [16].]

§ 3. — La norme, la différente, le discriminant d'un nombre. La base du corps.

Soit α un nombre quelconque du corps k et soient $\alpha', \ldots, \alpha^{(m-1)}$ les nombres conjugués à α, le produit

$$n(\alpha) = \alpha\alpha' \ldots \alpha^{(m-1)}$$

est dit la *norme* du nombre α. La norme d'un nombre α est toujours un nombre rationnel. De plus, le produit

$$\delta(\alpha) = (\alpha - \alpha')(\alpha - \alpha'') \ldots (\alpha - \alpha^{(m-1)})$$

est la *différente du nombre* α. La différente d'un nombre est encore un nombre du corps k.

Car si l'on pose

$$f(x) = (x - \alpha)(x - \alpha') \ldots (x - \alpha^{(m-1)}),$$

$$\delta(\alpha) = \left[\frac{df(x)}{dx}\right]_{x=\alpha}.$$

Enfin, le produit

$$d(\alpha) = (\alpha - \alpha')^2(\alpha - \alpha'')^2(\alpha' - \alpha'')^2 \ldots (\alpha^{(m-2)} - \alpha^{(m-1)})^2$$

$$= \begin{vmatrix} 1, & \alpha, & \alpha^2, & \ldots, & \alpha^{m-1} \\ 1, & \alpha', & \alpha'^2, & \ldots, & \alpha'^{m-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1, & \alpha^{(m-1)}, & (\alpha^{(m-1)})^2, & \ldots, & (\alpha^{(m-1)})^{m-1} \end{vmatrix}^2$$

est dit le *discriminant de* α.

Le discriminant d'un nombre rationnel est un nombre rationnel et au signe près il est égal à la norme de la différente ; en effet

$$d(\alpha) = (-1)^{\frac{m(m-1)}{2}} n(\delta).$$

Si α est un nombre qui détermine le corps, sa différente et son discriminant sont différents de zéro. Réciproquement, si la différente et le discriminant d'un nombre sont différents de zéro, ce nombre détermine le corps.

Si α est entier, sa norme, sa différente et son discriminant sont entiers.

THÉORÈME 5. — Dans tout corps de degré m, il existe m nombres entiers $\omega_1, \omega_2, \ldots, \omega_m$ tels que tout autre entier du corps ω puisse être représenté par

$$\omega = a_1\omega_1 + a_2\omega_2 + \ldots + a_m\omega_m,$$

où $a_1, a_2, \ldots, a_m$ sont des entiers rationnels.

Démonstration. — Si α est un nombre entier déterminant le corps, tout nombre ω est représentable par

$$\omega = r_1 + r_2\alpha + \ldots + r_m\alpha^{m-1},$$

où $r_1, r_2, \ldots, r_m$ sont des nombres rationnels.

En passant aux nombres conjugués

$$\omega' = r_1 + r_2\alpha' + \ldots + r_m\alpha'^{m-1},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\omega^{(m-1)} = r_1 + r_2\alpha^{(m-1)} + \ldots + r_m(\alpha^{(m-1)})^{m-1},$$

il en résulte pour $s = 1, 2, \ldots, m$

$$r_s = \frac{|1, \alpha, \ldots, \omega, \ldots, \alpha^{m-1}|}{|1, \alpha, \ldots, \alpha^{s-1}, \ldots, \alpha^{m-1}|^2} = \frac{A_s}{d(\alpha)},$$

où A_s comme fonction entière de $\alpha, \alpha', \ldots, \alpha^{(m-1)}, \omega, \omega', \ldots, \omega^{(m-1)}$ est un nombre entier. Comme, d'autre part, A_s est égal au nombre entier $r_s d(\alpha)$, A_s, d'après le théorème 4, est un nombre entier rationnel. Tout nombre entier ω peut donc être représenté par

$$(1) \qquad \omega = \frac{A_1 + A_2\alpha + \ldots + A_m\alpha^{m-1}}{d(\alpha)},$$

où $A_1, A_2, \ldots, A_m$ sont des entiers rationnels et où $d(\alpha)$ est le discriminant de α.

Soit à nouveau s un nombre de la suite $1, 2, \ldots, m$; supposons qu'on ait calculé tous les nombres du corps de la forme

$$\omega_s = \frac{O_1 + O_2\alpha + \ldots + O_s\alpha^{s-1}}{d(\alpha)},$$
$$\omega_s^{(1)} = \frac{O_1^{(1)} + O_2^{(1)}\alpha + \ldots + O_s^{(1)}\alpha^{s-1}}{d(\alpha)},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

où les $O, O^{(1)}, O^{(2)}, \ldots$ sont des nombres entiers rationnels, nous pouvons admettre que $O_s \neq 0$ et qu'il est le plus grand commun diviseur des $O_s, O_s^{(1)}, O_s^{(2)}, \ldots$ Alors les m premiers nombres correspondants $\omega_1, \ldots, \omega_m$ forment un système satisfaisant à la condition demandée. En effet, soit un nombre ω mis sous la forme (1); d'après ce que nous venons de dire, on devra avoir $A_m = a_m O_m$ où a_m est un nombre rationnel, mais alors la différence

$$\omega^* = \omega - a_m \omega_m$$

a la forme

$$\omega^* = \frac{A_1^* + A_2^* \alpha + \ldots + A_{m-1}^* \alpha^{m-2}}{d(\alpha)},$$

et l'on aura $A_{m-1} = a_{m-1} O_{m-1}$; si nous considérons la différence $\omega^{**} = \omega^* - a_{m-1}\omega_{m-1}$, et si nous poursuivons ce raisonnement, nous en concluerons l'exactitude du théorème (5).

Les nombres $\omega_1, \ldots, \omega_m$ forment ce que nous appellerons une base du système de tous les nombres entiers du corps k, ou tout simplement une *base du corps* k. Toute autre base du corps est donnée par les formules

$$\omega_1^* = a_{11}\omega_1 + \ldots + a_{1m}\omega_m,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$\omega_m^* = a_{m1}\omega_1 + \ldots + a_{mm}\omega_m$$

où le déterminant des coefficients $a = \pm 1$. [Dedekind [1], Kronecker [16].]

CHAPITRE II.

Les idéaux du corps.

§ 4. — La multiplication des idéaux et leur divisibilité. — L'idéal premier.

Le premier problème important de la théorie des corps algébriques est la recherche des lois de la décomposition (divisibilité) des nombres algébriques. Ces lois sont d'une admirable beauté et d'une grande simplicité. Elles présentent une analogie précise avec les lois élémentaires de la divisibilité pour les nombres entiers rationnels et elles ont la même signification fondamentale. Ces lois ont été découvertes d'abord par Kummer, mais le mérite de les avoir établies pour le corps algébrique général revient à Dedekind et à Kronecker.

Les principes fondamentaux de cette théorie sont les suivants :

Un système d'un nombre infini d'entiers algébriques $\alpha_1, \alpha_2, \ldots$ du corps k, tel que toute combinaison linéaire $\lambda_1\alpha_1 + \lambda_2\alpha_2 \ldots$ (où $\lambda_1, \lambda_2, \ldots$ sont des nombres entiers du corps) appartienne encore au système est dit un idéal $\mathfrak{a}$.

Théorème 6. — Dans chaque idéal $\mathfrak{a}$ il y a m nombres $i_1, i_2, \ldots, i_m$ tels que tout autre nombre de l'idéal est une combinaison linéaire

$$i = l_1 i_1 + \ldots + l_m i_m$$

où $l_1, \ldots, l_m$ sont des entiers rationnels.

Démonstration. — Soit s un des nombres $1, 2, \ldots, m$; imaginons qu'on ait calculé tous les nombres de l'idéal de la forme

$$\begin{aligned} i_s &= J_1\,\omega_1 + \ldots + J_s\omega_s, \\ i_1^{(1)} &= J_1^{(1)}\omega_1 + \ldots + J_s^{(1)}\omega_s, \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

où $J, J^{(1)}, \ldots$ sont des nombres entiers rationnels; admettons que $J_s \neq 0$ est le plus grand commun diviseur des nombres $J_s, J_s^{(1)}, \ldots$, on en déduira comme précédemment que les m nombres $i_1, \ldots, i_m$ satisfont à la condition indiquée.

Les nombres $i_1, \ldots, i_m$ sont dits la *base de l'idéal* $\mathfrak{a}$. Toute autre base de l'idéal peut être mise sous la forme

$$\begin{aligned} i_1^* &= a_{11}\,i_1 + \ldots + a_{1m}\,i_m, \\ i_m^* &= a_{m1}\,i_1 + \ldots + a_{mm}\,i_m, \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

où le déterminant de coefficients $a = \pm 1$.

Soient $\alpha_1, \ldots, \alpha_r$, r nombres de l'idéal $\mathfrak{a}$ tels que des combinaisons linéaires de ces nombres avec l'emploi de coefficients algébriques λ donnent tous les nombres de l'idéal, j'écrirai

$$\mathfrak{a} = (\alpha_1, \ldots, \alpha_r).$$

Si $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_r)$ et $\mathfrak{b} = (\beta_1, \ldots, \beta_s)$ sont deux idéaux, je désignerai par $(\mathfrak{a}, \mathfrak{b})$ l'idéal obtenu en réunissant les nombres $\alpha_1, \alpha_2, \ldots, \alpha_r; \beta_1, \beta_2, \ldots, \beta_s$, et j'écrirai

$$(\mathfrak{a}, \mathfrak{b}) = (\alpha_1, \ldots, \alpha_r; \beta_1, \ldots, \beta_s).$$

Un idéal qui contient tous les nombres de la forme $\lambda\alpha$ et ne contient que ces nombres où λ désigne un nombre entier quelconque appartenant au corps et α un nombre entier déterminé du corps est dit un *idéal principal;* on le désigne par (α), ou plus brièvement par α, dans le cas où il ne peut être confondu avec le nombre α.

Tout nombre α de l'idéal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ est dit *congru* à 0, suivant l'idéal $\mathfrak{a}$

$$\alpha \equiv 0 \qquad (\mathfrak{a}).$$

Lorsque la différence de α et β est congrue à 0 d'après $\mathfrak{a}$, on dit que α et β sont congrus suivant $\mathfrak{a}$; on écrit

$$\alpha \equiv \beta \qquad (\mathfrak{a});$$

sinon on dit qu'ils sont *incongrus*: on écrit

$$\alpha \not\equiv \beta \qquad (\mathfrak{a}).$$

Lorsqu'on multiplie chaque nombre d'un idéal $\mathfrak{a} = (\alpha_1, \ldots, \alpha_r)$ par chaque nombre d'un idéal $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_s)$ et que l'on combine linéairement les nombres ainsi obtenus au moyen de coefficients algébriques du corps, le nouvel idéal obtenu se nomme le *produit des deux idéaux* $\mathfrak{a}$ et $\mathfrak{b}$, c'est-à-dire

$$\mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \ldots, \alpha_r\beta_1, \ldots, \alpha_1\beta_s, \ldots, \alpha_r\beta_s).$$

Un idéal $\mathfrak{c}$ est dit *divisible* par l'idéal $\mathfrak{a}$, s'il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Si $\mathfrak{c}$ est divisible par $\mathfrak{a}$, tous les nombres de $\mathfrak{c}$ sont congrus à 0 suivant l'idéal $\mathfrak{a}$.

On a relativement aux diviseurs d'un idéal le théorème suivant :

LEMME 1. — Un idéal $\mathfrak{j}$ n'est divisible que par un nombre limité d'idéaux.

Démonstration. — Que l'on forme la norme n d'un nombre quelconque $\iota\ (\neq 0)$ de l'idéal $\mathfrak{j}$ et soit $\mathfrak{a}$ un diviseur de $\mathfrak{j}$, il est évident qu'alors le nombre rationnel entier $n \equiv 0$ suivant $\mathfrak{a}$. Supposons que les m nombres de base de $\mathfrak{a}$ soient de la forme

$$\alpha_1 = a_{11}\omega_1 + \ldots + a_{1m}\omega_m, \quad \ldots, \quad \alpha_m = a_{m1}\omega_1 + \ldots + a_{mm}\omega_m,$$

où $a_{11}, \ldots, a_{mm}$ sont des nombres entiers rationnels. Soient $a'_{11}, \ldots, a'_{mm}$ les plus petits restes possibles des nombres $a_{11}, \ldots, a_{mm}$ par n, on a :

$$\begin{aligned}\mathfrak{a} &= (a_{11}\omega_1 + \ldots + a_{1m}\omega_m, \quad \ldots, \quad a_{m1}\omega_1 + \ldots + a_{mm}\omega_m) \\ &= (a'_{11}\omega_1 + \ldots + a'_{1m}\omega_m, \quad \ldots, \quad a'_{m1}\omega_1 + \ldots + a_{mm}\omega_m, \ n)\end{aligned}$$

et cette dernière représentation de l'idéal $\mathfrak{a}$ montre l'exactitude de notre affirmation.

Un idéal différent de 1 et qui n'est divisible par aucun autre idéal que par lui-même et par l'unité est dit un *idéal premier*.

Deux idéaux sont dits *premiers* entre eux, si à part 1 ils ne sont divisibles en commun par aucun autre idéal.

Deux nombres entiers α et β, un nombre entier α et un idéal $\mathfrak{a}$ sont dits premiers si les idéaux principaux (α) et (β) ou si l'idéal principal (α) et $\mathfrak{a}$ sont premiers entre eux. [Dedekind[1].]

§ 5. Un idéal n'est décomposable que d'une seule manière en idéaux premiers.

On a le fait fondamental :

Théorème 7. — Tout idéal $\mathfrak{j}$ peut être décomposé en un produit d'idéaux premiers et il ne peut l'être que d'une seule manière.

Dedekind a donné récemment une nouvelle exposition de sa démonstration. [Dedekind[1].] La démonstration de Kronecker repose sur la théorie (créée par lui) des formes algébriques appartenant à un corps. La signification de cette théorie se comprend mieux, si l'on établit d'abord les théorèmes de la théorie des idéaux ; c'est alors que le lemme suivant rend de grands services.

Lemme 2. — Lorsque les coefficients de deux fonctions entières de la variable x :

$$F(x) = \alpha_1 x^r + \alpha_2 x^{r-1} + \ldots,$$
$$G(x) = \beta_1 x^s + \beta_2 x^{s-1} + \ldots$$

sont des nombres algébriques entiers et que les coefficients $\gamma_1, \gamma_2, \gamma_3, \ldots$ du produit

$$F(x)G(x) = \gamma_1 x^{r+s} + \gamma_2 x^{r+s-1} + \ldots$$

sont tous divisibles par le nombre entier ω, chacun des nombres $\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_2\beta_1, \alpha_2\beta_2$ est divisible par ω. [Kronecker[10], Dedekind[7], Mertens[1], Harwitz[1,2].]

De ce lemme on déduit successivement [Hurwitz[1]] :

Théorème 8. — A chaque idéal donné $\mathfrak{a} = (\alpha, \alpha_1, \ldots, \alpha_r)$, on peut faire correspondre un ideal $\mathfrak{b}$ tel que le produit $\mathfrak{a}\mathfrak{b}$ soit un idéal principal.

Démonstration. — Posons $F = \alpha_1 u_1 + \ldots + \alpha_r u_r$ et formons le produit des $m - 1$ formes avec les coefficients conjugués

$$R = (\alpha'_1 u_1 + \ldots + \alpha'_r u_r) \ldots (\alpha_1^{(m-1)} u_1 + \ldots + a_r^{(m-1)} u_r) = \beta_1 f_1 + \ldots + \beta_s f_s$$

où $f_1, \ldots, f_s$ sont certaines puissances différentes ou des produits de puissances des $u_1, u_2, \ldots, u_r$ et où $\beta_1, \beta_2, \ldots, \beta_r$ sont des nombres entiers du corps K, $FR = nU$ où n est un nombre entier rationnel et U une puissance entière à coefficients entiers, dont les coefficients n'ont pas de diviseur commun. Il en résulte que $n \equiv 0$ suivant le produit des deux idéaux $\mathfrak{a}$ et $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_s)$. Le lemme 2 nous montre que chaque nombre $\alpha_i\beta_h$ est divisible par n ; en appliquant ce lemme (2) aux deux fonctions obtenues lorsque dans F et R on pose

$$u_1 = x, \quad u_2 = x^{m-1}, \quad u_3 = x^{(m-1)^2}, \quad \ldots, \quad u_r = x^{(m-1)^{r-1}}.$$

On a donc

$$\mathfrak{a}\mathfrak{b} = n.$$

THÉORÈME 9. — Si l'on a pour les trois idéaux $\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c}$, $\mathfrak{ac} = \mathfrak{bc}$, on a aussi

$$\mathfrak{a} = \mathfrak{b}.$$

Démonstration. — Soit $\mathfrak{m}$ un idéal tel que $\mathfrak{cm}$ soit un idéal principal (α) d'après l'hypothèse

$$\mathfrak{acm} = \mathfrak{bcm},$$
$$\alpha\mathfrak{a} = \alpha\mathfrak{b},$$

et par suite

$$\mathfrak{a} = \mathfrak{b}.$$

THÉORÈME 10. — Si tous les nombres d'un idéal $\mathfrak{c}$ sont $\equiv 0$ suivant $\mathfrak{a}$, $\mathfrak{c}$ est divisible par $\mathfrak{a}$.

Demonstration. — Si $\mathfrak{am}$ est égal à l'idéal principal (α), tous les nombres $\mathfrak{mc}$ sont divisibles par α et par suite il existe un idéal tel que

$$\mathfrak{mc} = \alpha\mathfrak{b},$$

et par suite

$$\mathfrak{amc} = \alpha\mathfrak{ab},$$
$$\alpha\mathfrak{c} = \alpha\mathfrak{ab},$$
$$\mathfrak{c} = \mathfrak{ab}.$$

THÉORÈME 11. — Lorsque le produit de deux idéaux $\mathfrak{ab}$ est divisible par un idéal premier $\mathfrak{p}$, l'un des deux idéaux $\mathfrak{a}$ ou $\mathfrak{b}$ est divisible par $\mathfrak{p}$.

Démonstration. — Si $\mathfrak{a}$ n'est pas divisible par $\mathfrak{p}$, l'idéal $(\mathfrak{a}, \mathfrak{p})$ est différent de $\mathfrak{p}$ et de plus contenu dans $\mathfrak{p}$, c'est-à-dire $= 1$; d'après cela, on aurait $1 = \alpha + \pi$, où α est un nombre de $\mathfrak{a}$ et π un nombre de $\mathfrak{p}$; en multipliant par un nombre quelconque β de $\mathfrak{b}$, on aurait $\beta = \alpha\beta + \pi\beta \equiv \alpha\beta$ suivant $\mathfrak{p}$ par hypothèse, $\alpha\beta \equiv 0$ suivant $\mathfrak{p}$, par suite aussi $\beta \equiv 0$ suivant $\mathfrak{p}$.

Dès lors on démontre le théorème fondamental 7 de la théorie des idéaux ainsi qu'il suit :

Si $\mathfrak{j}$ n'est pas un idéal premier, on a $\mathfrak{j} = \mathfrak{ab}$ où $\mathfrak{a}$ est un diviseur de $\mathfrak{j}$ différent de $\mathfrak{j}$ et de 1. Si l'un des facteurs $\mathfrak{a}$ ou $\mathfrak{b}$ n'est pas un idéal premier, nous le représenterons lui-même comme un produit d'idéaux et nous aurons $\mathfrak{j} = \mathfrak{a}'\mathfrak{b}'\mathfrak{c}'$ et nous continuerons ainsi. Nous ne pourrons pas continuer indéfiniment, car, d'après le lemme 1, un idéal n'admet qu'un nombre fini de diviseurs. Soit r ce nombre, $\mathfrak{j}$ ne peut être le produit de plus de r facteurs, car si

$$\mathfrak{j} \text{ était } = \mathfrak{a}_1 \times \mathfrak{a}_2 \times \ldots \times \mathfrak{a}_{r+1}$$

il serait divisible par les $r + 1$ idéaux différents

$$\mathfrak{a}_1, \quad \mathfrak{a}_1\mathfrak{a}_2, \quad \ldots, \quad \mathfrak{a}_1 \ldots \mathfrak{a}_{r+1}.$$

La représentation

$$\mathfrak{j} = \mathfrak{p}\mathfrak{q} \ldots \mathfrak{l}$$

n'est possible que d'une seule manière, car si l'on avait

$$\mathfrak{j} = \mathfrak{p}'\mathfrak{q}' \ldots \mathfrak{l}',$$

$\mathfrak{j}$ serait divisible par $\mathfrak{p}'$, et par suite aussi l'un des facteurs du premier produit (théorème 11) on aurait $\mathfrak{p} = \mathfrak{p}'$, et par suite d'après le théorème 9

$$\mathfrak{q} \ldots \mathfrak{l} = \mathfrak{q}' \ldots \mathfrak{l}';$$

on continuerait de la même manière.

Nous déduirons du théorème fondamental :

Théorème 12. — Tout idéal $\mathfrak{j}$ d'un corps k peut être représenté comme le plus grand commun diviseur de deux nombres entiers du corps $\varkappa$ et ρ.

Démonstration. — Soit $\varkappa$ un nombre divisible par $\mathfrak{j}$ et ρ un nombre divisible par $\mathfrak{j}$, mais tels que $\frac{\varkappa}{\mathfrak{j}}$ et $\frac{\rho}{\mathfrak{j}}$ soient premiers entre eux, on a $\mathfrak{j} = (\varkappa, \rho)$.

§ 6. — Les formes des corps algébriques et leurs contenus.

La théorie des formes de Kronecker [Kronecker[16]] exige d'autres formations :

Une fonction entière rationnelle F d'un nombre quelconque de variables, dont les coefficients sont des nombres algébriques entiers du corps k, est dite une *forme du corps k*. Si l'on substitue dans la forme F aux coefficients successivement tous leurs nombres conjugués et si l'on fait le produit des *formes conjuguées* ainsi obtenues $F', \ldots, F^{m-1}$ et de la forme F, on obtient une forme entière des variables $u, v, \ldots$, dont les coefficients sont des entiers rationnels; prenons-la sous la forme $nU(u, v, \ldots)$, où n est un entier rationnel et U une fonction entière rationnelle, dont les coefficients sont des entiers rationnels sans diviseur commun, n s'appelle la *norme de la forme* F. Lorsque la norme n est égale à 1, la forme se nomme une *forme unité*. Une fonction entière, dont les coefficients sont des entiers rationnels sans diviseur commun, est dite *forme unité rationnelle*. Deux formes sont dites *équivalentes* (ce qui s'exprime par le signe $\sim$) lorsque leur quotient est égal au quotient de deux formes unités (1); en particulier, toute forme unité ~ 1. Une forme H est dite *divisible* par une forme G s'il existe une forme G telle que $H \simeq FG$. Une forme P est dite une *forme première* lorsque P, dans le sens restreint, n'est divisible que par elle-même et par 1.

Le rapport de la théorie des formes de Kronecker avec la théorie des idéaux

(1) Kronecker emploie l'expression « équivalente au sens restreint ».

devient claire par la remarque que de chaque idéal $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ on peut tirer une forme F, et cela en multipliant les nombres $\alpha_1, \ldots, \alpha_r$ par des produits différents de puissances d'indéterminées $u, v, \ldots$ et en additionnant ces produits. Réciproquement, chaque forme de coefficients $\alpha_1, \ldots \alpha_r$ fournit un idéal $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$. C'est cet idéal que l'on nomme *contenu* de la forme F.

On a alors :

THÉORÈME 13. — Le contenu du produit de deux formes est égal au produit de leurs contenus.

Démonstration. — Soient F et G des formes d'un nombre quelconque de variables et soient $\alpha_1, \ldots, \alpha_r$ et $\beta_1, \ldots, \beta_s$ leurs coefficients respectifs. Soit $H=FG$ une forme de coefficients $\gamma_1, \ldots, \gamma_t$. De plus, soit $\mathfrak{p}^a$ la plus haute puissance de l'idéal premier $\mathfrak{p}$ contenu dans $\mathfrak{a}=(\alpha_1, \ldots, \alpha_r)$ et $\mathfrak{p}^b$ la plus haute puissance de $\mathfrak{p}$ contenu dans $\mathfrak{b}=(\beta_1, \ldots, \beta_s)$. Supposons qu'on ait ordonné les termes de F et de G d'après les puissances décroissantes de u, puis les termes contenant les mêmes puissances de a d'après les puissances décroissantes de v, et ainsi de suite. Soit alors $\alpha u^h v^l \ldots$ le premier terme de F dont le coefficient n'est pas divisible par une puissance de $\mathfrak{p}$ supérieure à la $a^{\text{ème}}$, et, d'autre part, $\beta u^{h'} v^{l'} \ldots$ le premier terme de b dont le coefficient n'est pas divisible par une puissance de $\mathfrak{p}$ supérieure à la $b^{\text{ème}}$, il est évident que le coefficient γ du terme $\gamma u^{h+h'} v^{l+l'} \ldots$ de H ne sera pas divisible par une puissance de $\mathfrak{p}$ supérieure à la $(a+b)^{\text{ème}}$. Tous les autres coefficients de H seront certainement divisibles par $\mathfrak{p}^{a+b}$. Il en résulte que

$$(\alpha_1, \ldots, \alpha_r)(\beta_1, \ldots, \beta_s)=(\gamma_1, \ldots, \gamma_t).$$

De 13 il résulte facilement que toute forme unité a pour contenu 1, et que réciproquement toute forme dont les coefficients ont pour plus grand commun diviseur idéal l'unité est une forme unité. Il en résulte aussi que deux formes équivalentes ont le même contenu et que toutes les formes de même contenu sont équivalentes.

On a d'autres conséquences du théorème 13.

THÉORÈME 14. — A toute forme donnée F on peut adjoindre une forme R telle que le produit FR soit égal à un nombre entier.

THÉORÈME 15. — Lorsque le produit de deux formes est divisible par une forme première, l'une des formes au moins est divisible par P.

THÉORÈME 16. — Toute forme peut être (dans le sens de l'équivalence) décomposée en produit de formes premières et ne peut l'être que d'une manière. Ces théorèmes sont parallèles aux théorèmes 8 et 11 et au théorème 7, théorème fondamental de la théorie des idéaux.

A part les méthodes suivies par Dedekind et Kronecker, il existe encore deux méthodes plus simples pour démontrer le théorème fondamental 7; la théorie des nombres de Galois est la base de l'une. Voir § 36. [Hilbert[12].]

La deuxième méthode est fondée sur ce théorème que les idéaux d'un corps se répartissent en un nombre limité de classes. L'idée principale de la démonstration de ce théorème peut être considérée comme la généralisation de la marche suivie pour déterminer le plus grand commun diviseur de deux nombres, d'après la méthode d'Euclide. [Hurwitz[3].]

CHAPITRE III.

Les congruences suivant les idéaux.

§ 7. — La norme d'un idéal et ses propriétés.

La théorie exposée au chapitre II sur la décomposition des idéaux en facteurs nous permet d'étendre la théorie des nombres rationnels aux nombres d'un corps algébrique.

Nous exposerons d'abord les notions et les théorèmes suivants :

Le nombre des entiers incongrus l'un à l'autre suivant l'idéal $\mathfrak{a}$ d'un corps k est dit la *norme de l'idéal* $\mathfrak{a}$; il s'écrit $n(\mathfrak{a})$.

Théorème 17. — La norme de l'idéal premier $\mathfrak{p}$ est une puissance du nombre rationnel p divisible par $\mathfrak{p}$.

Démonstration. — Soient les f nombres entiers $\omega_1, \ldots, \omega_f$ d'une base du corps k indépendants l'un de l'autre, en ce sens qu'entre ces nombres il n'existe aucune congruence de la forme

$$a_1\omega_1 + \ldots + a_f\omega_f \equiv 0 \qquad (\mathfrak{p})$$

où $a_1, \ldots, a_f$ sont des entiers rationnels non tous divisibles par p, et supposons de plus que chacun des $m-f$ autres nombres de la base soit congru à une expression de la forme

$$a_1\omega_1 + \ldots + a_f\omega_f$$

suivant le module $\mathfrak{p}$; cette expression pourra être congrue suivant $\mathfrak{p}$ à un nombre quelconque, et le nombre des nombres incongrus suivant $\mathfrak{p}$ sera $\mathfrak{p}^f$; f est dit le degré de l'idéal premier $\mathfrak{p}$.

Théorème 18. — La norme du produit $\mathfrak{a}\mathfrak{b}$ de deux idéaux est égal au produit de leurs normes.

Démonstration. — Soit α un nombre divisible par $\mathfrak{a}$ tel que $\frac{\alpha}{\mathfrak{a}}$ soit un idéal premier avec $\mathfrak{b}$. Si ξ parcourt un système de $n(\mathfrak{a})$ nombres incongrus suivant $\mathfrak{a}$, et η un système de $n(\mathfrak{b})$ nombres incongrus suivant $\mathfrak{b}$, le nombre $\alpha\eta + \xi$ représentera un système complet de nombres incongrus suivant $\mathfrak{a}\mathfrak{b}$; un pareil système comprend $n(\mathfrak{a})\,n(\mathfrak{b})$ nombres.

Théorème 19. — Lorsque

$$\begin{array}{l} i_1 = a_{11}\omega_1 + \ldots + a_{1m}\omega_m, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ i_m = a_{m1}\omega_1 + \ldots + a_{mm}\omega_m \end{array}$$

représente une base de l'idéal $\mathfrak{a}$, la norme $n(\mathfrak{a})$ est égale à la valeur absolue du déterminant des coefficients a.

Démonstration. — Mettons la base de l'idéal sous la forme trouvée dans la démonstration du théorème 6, où tous les coefficients a_{rs} sont $= 0$ pour $s > r$, le déterminant des coefficients est alors

$$a_{11}a_{22}\ldots a_{mm}.$$

D'autre part, l'expression

$$u_1\omega_1 + \ldots + u_m\omega_m$$

où

$$u_1 = 0,\quad 1,\quad \ldots,\quad a_{11} - 1,\quad \ldots,\quad u_m = 0,\quad 1,\quad \ldots,\quad a_{mm} - 1$$

représente un système complet de nombres incongrus à $\mathfrak{a}$, ce qui démontre le théorème 19. De plus, on voit que la réciproque est vraie. Les rapports de ce qui précède avec la théorie des formes de Kronecker résultent du

Théorème 20. — Soit F une forme qui a pour contenu $\mathfrak{a}$, la norme de la forme F est égale à la norme de l'idéal $\mathfrak{a}$, c'est-à-dire $n(\mathrm{F}) = n(\mathfrak{a})$. En particulier, la norme d'un entier α est égale à la valeur absolue de la norme de l'idéal principal $\mathfrak{a} = (\alpha)$.

Démonstration. — Soient $i_1, \ldots, i_m$ une base de l'idéal $\mathfrak{a}$; construisons une forme F

$$\mathrm{F} = i_1 u_1 + \ldots + i_m u_m ;$$

alors

$$\begin{array}{l} \omega_1 \mathrm{F} = l_{11}\, i_1 + \ldots + l_{1m}\, i_m, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \omega_m \mathrm{F} = l_{m1}\, i_1 + \ldots + l_{mm}\, i_m \end{array}$$

où $l_{11}, \ldots, l_{mm}$ sont les formes linéaires des $u_1, \ldots, u_m$ à coefficients entiers et rationnels. Nous démontrerons tout d'abord que le déterminant $[l_{rs}]$ des formes $l_{11}, \ldots, l_{mm}$ est une forme unité rationnelle.

En effet, car si au contraire tous les coefficients du déterminant $[l_{rs}]$ étaient divisibles par un nombre premier p, il exciterait au moins m formes $L_1, \ldots, L_m$, dont les coefficients sont des entiers rationnels, non tous divisibles par p, et tels que

$$L_1 l_{11} + \ldots + L_m l_{m1} \equiv 0 \qquad (p),$$
$$\ldots\ldots\ldots\ldots$$
$$L_1 l_{1m} + \ldots + L_m l_{mm} \equiv 0 \qquad (p).$$

Il en résulterait

$$(L_1 \omega_1 + \ldots + L_m \omega_m) F \equiv 0, \qquad (p\mathfrak{a})$$

c'est-à-dire que le produit $\mathfrak{l}\mathfrak{a}$ serait divisible par $p\mathfrak{a}$ où $\mathfrak{l}$ désigne le contenu de la forme $L_1\omega_1 + \ldots + L_m\omega_m$, et par suite $\mathfrak{l}$ serait divisible par p, ce qui n'est pas possible, car un nombre de la forme $a_1\omega_1 + \ldots + a_m\omega_m$ où $a_1, \ldots, a_m$ sont des entiers rationnels ne peut être divisible par p que si tous les coefficients $a_1, \ldots, a_m$ le sont.

D'après le théorème de la multiplication des déterminants

$$\begin{vmatrix} \omega_1 F, & \ldots, & \omega_m F \\ \omega'_1 F', & \ldots, & \omega'_m F' \\ \ldots & \ldots & \ldots \\ \omega_1^{(m-1)} F^{(m-1)}, & \ldots, & \omega_m^{(m-1)} F^{(m-1)} \end{vmatrix} = \begin{vmatrix} l_{11}, & \ldots, & l_{1m} \\ l_{21}, & \ldots, & l_{2m} \\ \ldots & \ldots & \ldots \\ l_{m1}, & \ldots, & l_{mm} \end{vmatrix} \times \begin{vmatrix} i_1, & \ldots, & i_m \\ i'_1, & \ldots, & i'_m \\ \ldots & \ldots & \ldots \\ i_1^{(m-1)}, & \ldots, & i_m^{(m-1)} \end{vmatrix}$$

et en divisant par le facteur

$$\begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega'_1, & \ldots, & \omega'_m \\ \ldots & \ldots & \ldots \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}$$

on a la relation

$$FF' \ldots F^{m-1} \simeq n(\mathfrak{a}),$$
$$n(F) = n(\mathfrak{a}).$$

La deuxième partie du théorème est évidente pour $F = \alpha$.

Si l'on applique à tous les nombres $\alpha_1, \alpha_2, \ldots$ de l'idéal $\mathfrak{a}$ la substitution $t' = (\theta : \theta')$, l'idéal $\mathfrak{a}'$ qui résulte de l'idéal $\mathfrak{a}$ par la substitution t', $\mathfrak{a} = (t'\alpha_1, t'\alpha_2 \ldots)$, s'appelle *l'idéal conjugué* de $\mathfrak{a}$.

Si l'on considère le corps composé de $k, k', \ldots, k^{m-1}$, les théorèmes 18 et 20 nous apprennent que le produit de $\mathfrak{a}$ et de tous les idéaux conjugués à $\mathfrak{a}$ est égal à un nombre entier rationnel $n(\mathfrak{a})$.

De là découle une nouvelle définition de la norme d'un idéal $\mathfrak{a}$ qui correspond à la définition de la norme d'un nombre entier et qui est susceptible d'une importante généralisation. (Voir § 14.)

Théorème 21. — Dans tout idéal $\mathfrak{j}$ il existe deux nombres dont les normes ont pour plus grand diviseur la norme de $\mathfrak{j}$.

Démonstration. — Soit $a = n(\mathfrak{j})$ et soit α un nombre de $\mathfrak{j}$ tel que $\frac{\alpha}{\mathfrak{j}}$ soit premier avec a. Alors si $\alpha', \ldots, \alpha^{(m-1)}$ sont les nombres conjugués de α et $\mathfrak{j}', \ldots, \mathfrak{j}^{(m-1)}$ les idéaux conjugués de $\mathfrak{j}$, $\frac{\alpha'}{\mathfrak{j}'}, \ldots, \frac{\alpha^{(m-1)}}{\mathfrak{j}^{(m-1)}}$ et par suite $\frac{n(\alpha)}{n(\mathfrak{j})} = \frac{n(\alpha)}{a}$ seront premiers avec a, c'est-à-dire que

$$n(\mathfrak{j}) = a = \left(a^m, n(\alpha)\right) = \left(n(a), n(\alpha)\right).$$

§ 8. — Le théorème de Fermat dans la théorie des idéaux et la fonction $\varphi(\mathfrak{a})$.

En s'appuyant sur les mêmes conclusions que dans la théorie des nombres rationnels, on obtient le fait suivant correspondant au théorème de Fermat. [Dedekind [1].]

Théorème 22. — Si $\mathfrak{p}$ est un idéal premier de degré f, tout nombre entier ω du corps satisfait à la congruence

$$\omega^{p^f} \equiv \omega, \qquad (\mathfrak{p}).$$

Le théorème de Fermat généralisé se transporte aussi facilement dans la théorie des corps. On démontre sans peine les théorèmes suivants. [Dedekind [1].]

Théorème 23. — Le nombre des nombres incongrus suivant l'idéal $\mathfrak{a}$ et premier avec $\mathfrak{a}$ est

$$\varphi(\mathfrak{a}) = n(\mathfrak{a})\left(1 - \frac{1}{n(\mathfrak{p}_1)}\right)\left(1 - \frac{1}{n(\mathfrak{p}_2)}\right)\cdots\left(1 - \frac{1}{n(\mathfrak{p}_r)}\right)$$

où $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ sont les idéaux premiers différents qui divisent $\mathfrak{a}$. On a pour le nombre φ les formules

$$\varphi(\mathfrak{a})\varphi(\mathfrak{b}) = \varphi(\mathfrak{a}\mathfrak{b}),$$

bien entendu si $\mathfrak{a}$ et $\mathfrak{b}$ sont premiers entre eux :

$$\Sigma\varphi(\mathfrak{t}) = n(\mathfrak{a});$$

dans cette dernière formule la sommation s'étend à tous les idéaux $\mathfrak{t}$ diviseurs de $\mathfrak{a}$.

Théorème 24. — Chaque nombre entier ω premier avec un idéal $\mathfrak{a}$ satisfait à la congruence

$$\omega^{\varphi(\mathfrak{a})} \equiv 1 \qquad (\mathfrak{a}).$$

Ainsi chaque nombre entier qui n'est pas divisible par un idéal premier de degré f satisfait à

$$\omega^{p^f(p^f-1)} \equiv 1 \qquad (\mathfrak{p}^2).$$

On a de plus les faits suivants :

Théorème 25. — Si $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ sont des idéaux premiers entre eux deux à deux et si $\alpha_1, \ldots, \alpha_r$ sont des entiers quelconques, il y a toujours un nombre entier ω satisfaisant aux congruences

$$\omega \equiv \alpha_1, \quad (\mathfrak{a}_1), \quad \ldots, \quad \omega \equiv \alpha_r, \qquad (\mathfrak{a}_r).$$

Théorème 26. — Une congruence de degré r suivant l'idéal $\mathfrak{p}$ de la forme

$$\alpha x^r + \alpha_1 x^{r-1} + \ldots + \alpha_r \equiv 0 \qquad (\mathfrak{p})$$

où $\alpha, \alpha_1, \ldots, \alpha_r$ sont des nombres entiers, admet au plus r racines incongrues d'après $\mathfrak{p}$.

Théorème 27. — Soit $\mathfrak{p}$ un idéal premier diviseur du nombre premier rationnel p et soit α une racine de la congruence

$$a x^r + a_1 x^{r-1} + \ldots + a_r \equiv 0 \qquad (\mathfrak{p})$$

où $a, a_1, \ldots, a_r$ sont des nombres entiers rationnels, α^p est aussi racine de cette congruence.

Démonstration. — Désignons le premier membre de la congruence par $\mathrm{F}x$; on a, d'après le théorème de Fermat, la congruence identique en x,

$$\mathrm{F}(x^p) \equiv \big(\mathrm{F}(x)\big)^p \quad \text{suivant } \mathfrak{p},$$

ce qui implique le théorème.

§ 9. — Les nombres primitifs suivant un idéal premier.

Un nombre entier ρ du corps k est dit un nombre primitif *suivant l'idéal premier* $\mathfrak{p}$ si les $p^f - 1$ premières puissances de ce nombre représentent $p^f - 1$ nombres incongrus suivant $\mathfrak{p}$ premiers avec $\mathfrak{p}$. En procédant comme pour les nombres rationnels, on arrive facilement à démontrer les faits suivants.

Théorème 28. — Il y a $\Phi(p^f - 1)$ nombres primitifs pour l'idéal premier $\mathfrak{p}$ où $\Phi(p^f - 1)$ désigne le nombre des restes rationnels incongrus suivant $p^f - 1$ et premiers avec $p^f - 1$.

On n'a pas encore développé une théorie des nombres primitifs pour les puissances d'un idéal premier $\mathfrak{p}$; mais on reconnaît sans peine les résultats suivants. [Dedekind[6].]

Théorème 29. — Soit $\mathfrak{p}$ un idéal premier quelconque du corps k, on peut toujours trouver dans k un nombre ρ tel que tout autre nombre du corps soit congru à une certaine fonction de ρ à coefficients entiers rationnels suivant une puissance $\mathfrak{p}^l$ de l'idéal premier $\mathfrak{p}$, quel que soit l.

Démonstration. — Soit ρ^* un nombre primitif quelconque de $\mathfrak{p}$, il est évident que tous les nombres entiers sont congrus à certaines fonctions à coefficients entiers de ρ^* suivant $\mathfrak{p}$. Soit

$$P(\rho^*) \equiv 0 \qquad (\mathfrak{p})$$

la congruence de degré la moins élevée à laquelle satisfait ρ^*.

Si le degré de la fonction $P = f'$, aucune expression de la forme

$$a_1 + a_2\rho^* + \ldots + a_{f'}\rho^{*f'-1}$$

à coefficients entiers $a_1, a_2, \ldots, a_{f'}$ ne peut être congrue à o d'après $(\mathfrak{p})$; à moins que tous ses coefficients $a_1, a_2, \ldots, a_{f'}$ ne soient congrus à o d'après p. Comme, d'autre part, tout nombre entier du corps est une expression de cette forme, il en résulte $f' = f$.

Dans le cas où $P(\rho^*) \equiv 0$ suivant $\mathfrak{p}^2$, on posera $\rho = \rho^* + \pi$, où π est divisible par $\mathfrak{p}$ et non par $\mathfrak{p}^2$. On a alors à cause de $\dfrac{dP(\rho^*)}{d\rho^*} \not\equiv 0$, suivant $\mathfrak{p}$ nécessairement,

$$P(\rho) = P(\rho^* + \pi) = P(\rho^*) + \pi \frac{dP(\rho^*)}{d\rho^*} \not\equiv 0, \qquad (\mathfrak{p}).$$

ρ est un nombre ayant la propriété demandée, car si $\alpha_1, \alpha_2, \ldots, \alpha_l$ parcourent toutes les expressions de la forme $a_1 + a_2\rho + \ldots + a_f r^{f-1}$, où $a_1, a_2, \ldots, a_f$ sont des nombres de la suite o, 1, ..., $p-1$, la somme $\alpha_1 + \alpha_2 P(\rho) + \ldots + \alpha_e [P(\rho)]^{l-1}$ représente des nombres incongrus par rapport à $\mathfrak{p}^l$, et comme il y a ici p^{fl} nombres, on a épuisé les restes incongrus d'après $\mathfrak{p}^l$.

Il est évident que tout nombre congru à ρ suivant $\mathfrak{p}^2$ possède la même propriété. Nous utiliserons cette dernière circonstance pour représenter un idéal $\mathfrak{p}$.

Théorème 30. — Étant donné un idéal $\mathfrak{p}$ de degré f, il y a toujours dans le corps k un nombre ρ entier satisfaisant au théorème 29 et de plus tel que

$$\mathfrak{p} = \big(p, P(\rho)\big)$$

où $P(\rho)$ est une fonction entière de degré f de ρ à coefficients rationnels et entiers.

Démonstration. — Soit $p = \mathfrak{p}^l\mathfrak{a}$ où l'idéal $\mathfrak{a}$ n'est pas divisible par $\mathfrak{p}$. De plus, soit α un nombre entier non divisible par $\mathfrak{p}$ mais divisible par $\mathfrak{a}$. D'après le théorème 24, $\alpha^{p^f(p^f-1)} \equiv 1$ suivant $\mathfrak{p}^2$. Remplaçons le nombre ρ trouvé tout à l'heure par $\rho\alpha^{p^f(p^f-1)}$; le nombre ρ conserve sa propriété précédente; comme de plus le dernier coefficient de $P(\rho)$ n'est pas divisible par p, pour le nouveau nombre ρ $P(\rho)$ est premier avec $\mathfrak{a}$, de sorte que

$$\mathfrak{p} = \big(p, P(\rho)\big).$$

CHAPITRE IV.

Le discriminant du corps et ses diviseurs.

§ 10. — Le théorème relatif aux diviseurs du discriminant du corps. Théorèmes auxiliaires pour les fonctions entières.

Le *discriminant* du corps k est défini par

$$d = \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega'_1, & \ldots, & \omega'_m \\ \cdot & \cdot & \cdot \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}^2$$

où $\omega_1, \omega_2, \ldots, \omega_m$ est une base du corps; le discriminant est un nombre entier rationnel. La recherche des diviseurs idéaux de d a une importance fondamentale dans le développement de la théorie des corps. On a le théorème fondamental suivant :

Théorème 31. — Le discriminant d du corps contient comme facteurs premiers rationnels tous les nombres premiers rationnels divisibles par le carré d'un idéal premier et ne contient que ceux-là.

La démonstration de ce théorème présentait de sérieuses difficultés, Dedekind parvint à les surmonter pour la première fois. [Dedekind[6].]

Hensel a donné une deuxième démonstration de ce théorème qui complète sur un point important la théorie de Kronecker relative aux nombres algébriques. La démonstration de Hensel repose sur les concepts suivants créés par Kronecker. [Kronecker[16], Hensel[4].]

Soient $u_1, \ldots, u_m$ des indéterminées et $\omega_1, \ldots, \omega_m$ une base, la forme

$$\xi = \omega_1 u_1 + \ldots + \omega_m u_m$$

est dite la *forme fondamentale* du corps k; elle satisfait à l'équation en x,

$$(x - \omega_1 u_1 - \ldots - \omega_m u_m)(x - \omega'_1 u_1 - \ldots - \omega'_m u_m) \ldots (x - \omega_1^{(m-1)} u_1 - \ldots - \omega_m^{(m-1)} u_m) = 0,$$

qu'on peut écrire

$$x^m + U_1 x^{m-1} + U_2 x^{m-2} + \ldots + U_m = 0$$

où $U_1, \ldots, U_m$ sont des fonctions de $u_1, \ldots, u_m$ à coefficients entiers et rationnels. Cette équation de degré m est dite l'*équation fondamentale*. Pour pouvoir opérer avec

les concepts que l'on vient de définir, il est nécessaire d'étendre les théorèmes sur la décomposition des fonctions entières d'une variable x suivant un nombre rationnel premier p [Serret[1]] au cas plus général où les fonctions entières contiennent en plus de la variable x les m paramètres indéterminés $u_1, u_2, \ldots, u_m$.

Dans ce qui suit, nous entendrons toujours par *fonction à coefficients entiers* une fonction rationnelle entière de la variable et des indéterminées dont les coefficients sont des *nombres entiers rationnels*. De plus, nous dirons qu'une fonction entière $Z(x; u_1, \ldots, u_m)$ est *divisible* suivant p par une autre fonction entière X, s'il existe une troisième fonction entière Y, telle que la congruence

$$Z \equiv XY \qquad (p)$$

ait lieu identiquement par rapport aux variables $x, u_1, \ldots, u_m$.

Lorsqu'une fonction entière à coefficients entiers n'est divisible suivant le module p que par des fonctions congrues à un nombre rationnel ou à la fonction P elle-même suivant p, nous dirons que la fonction P est *irréductible suivant le module p*, ou encore qu'elle est *première suivant le module p* (*Primfunction*).

Les théorèmes relatifs à la divisibilité se démontrent comme dans la théorie des fonctions d'une seule variable; nous ferons remarquer en particulier le théorème suivant que l'on démontre facilement par la récurrence euclidienne.

Théorème 32. — Lorsque deux fonctions entières à coefficients entiers X et Y de $x, u_1, \ldots, u_m$ n'ont pas de diviseur commun suivant le module p, il existe une fonction U entière à coefficients entiers de $u_1, \ldots, u_m$ seulement non congrue à o suivant p, telle que

$$U \equiv AX + BY \qquad (p),$$

où A et B sont des fonctions convenablement calculées de $x, u_1, u_2, \ldots, u_m$.

Notre but est de décomposer le premier membre F de l'équation fondamentale en fonctions irréductibles suivant le module p. Nous démontrerons tout d'abord les lemmes suivants :

Lemme 3. — Soit $\mathfrak{p}$ un idéal premier diviseur de p et de degré f; on peut toujours construire une fonction $H(x; u_1, u_2, \ldots, u_m)$ de degré f en x irréductible suivant p et qui, lorsqu'on y remplace x par la forme fondamentale ξ, a les propriétés suivantes : les coefficients des puissances et produits des $u_1, u_2, \ldots, u_m$ dans cette fonction sont tous divisibles par $\mathfrak{p}$ et ne le sont pas par $\mathfrak{p}^2$, et ils ne sont pas tous divisibles par un idéal premier différent de $\mathfrak{p}$ et diviseur de p.

Démonstration. — Soit $p = \mathfrak{p}^e \mathfrak{a}$, $\mathfrak{a}$ n'étant plus divisible par $\mathfrak{p}$. De plus, soit ρ une racine primitive de $\mathfrak{p}$ qui a les propriétés indiquées par les théorèmes 29 et 30, et soit $P(\rho)$ une fonction déterminée comme il a été dit, elle est entière à coefficients entiers de degré f, elle appartient à $\mathfrak{p}$ et telle que $\mathfrak{p} = (p, P(\rho))$.

P(x) est irréductible suivant p, sans quoi ρ satisferait à une congruence suivant $\mathfrak{p}$ de degré inférieur à f. Posons

$$\rho = a_1\omega_1 + \ldots + a_m\omega_m$$

où $a_1, \ldots, a_m$ sont des entiers rationnels, et nous admettrons que le coefficient de ρ^f dans P(ρ) est $= 1$. Comme on a

$$P(\rho) \equiv 0 \qquad (\mathfrak{p})$$

d'après le théorème 27, on a aussi

$$P(\rho^p) \equiv 0, \quad P(\rho^{p^2}) \equiv 0, \quad \ldots, \quad P(\rho^{p^{f-1}}) \equiv 0 \qquad (\mathfrak{p}),$$

c'est-à-dire que la congruence $P(x) \equiv 0$ ($\mathfrak{p}$) admet les f racines incongrues

$$\rho, \rho^p, \ldots, \rho^{p^{f-1}}$$

et on a identiquement

$$P(x) \equiv (x-\rho)(x-\rho^p)\ldots(x-\rho^{p^{f-1}}) \qquad (\mathfrak{p}),$$

c'est-à-dire que les fonctions symétriques élémentaires de $\rho, \rho^p, \ldots, \rho^{p^{f-1}}$ sont congrues suivant $\mathfrak{p}$ à certains nombres entiers rationnels.

Comme tout nombre entier du corps k est congru suivant $\mathfrak{p}$ à une fonction entière à coefficients entiers de ρ, nous pouvons poser

$$\xi \equiv L(\rho; u_1, \ldots; u_m)$$

suivant $\mathfrak{p}$, L fonction à coefficients entiers de $\rho, u_1, u_2, \ldots, u_m$.

D'après ce qu'on vient de lire, l'expression

$$[x - L(\rho; u_1, \ldots, u_m)][x - L(\rho^p; u_1, \ldots, u_m)] \ldots [x - L(\rho^{p^{f-1}}; u_1, \ldots, u_m)]$$

est congrue suivant $\mathfrak{p}$ à une fonction entière à coefficients entiers de $x, u_1, u_2, \ldots, u_m$; nous la mettrons sous la forme

$$\Pi(x; u_1, \ldots, u_m) = x^f + V_1 x^{f-1} + \ldots + V_f$$

où $V_1, \ldots, V_f$ sont des fonctions entières à coefficients entiers de $u_1, u_2, \ldots, u_m$. Il est évident que ξ mis à la place de x satisfait à

$$\Pi(x; u_1, \ldots, u_m) \equiv 0 \qquad (\mathfrak{p}).$$

Comme la fonction $\Pi(x; u_1, \ldots, u_m) \equiv P(x)$ suivant $\mathfrak{p}$, il en résulte que

$$\mathfrak{p} = \big(p, \Pi(\rho; u_1, \ldots, u_m)\big)$$

et que par suite les coefficients des puissances et produits de $u_1, \ldots, u_m$ dans $\Pi(\xi; u_1, \ldots, u_m)$ ne sont pas tous divisibles par $\mathfrak{p}^2$ et pas tous par un idéal premier différent de $\mathfrak{p}$ et contenu dans $\mathfrak{a}$.

LEMME 4. — Toute fonction entière $\Phi(x; u_1, \ldots, u_m)$ à coefficients entiers qui est identiquement congrue à o ($\mathfrak{p}$) lorsqu'on remplace x par la forme fondamentale ξ est divisible suivant p par la fonction $\Pi(x; u_1, \ldots, u_m)$.

Démonstration. — Dans le cas contraire, Φ et Π n'aurait pas de diviseur commun suivant p, et d'après le théorème 32 il y aurait une fonction U à coefficients entiers des suites variables $u_1, u_2, \ldots, u_m$ non congrue à zéro suivant p, telle que

$$U \equiv A\Phi + B\Pi \quad \text{suivant } \mathfrak{p},$$

A et B étant des fonctions à coefficients entiers de $x, u_1, u_2, \ldots, u_m$. D'après cela, en remplaçant x par ξ, on aurait $U \equiv$ o suivant $\mathfrak{p}$ et par suite suivant p, ce qui est contraire à l'hypothèse.

LEMME 5. — Si Φ est une fonction à coefficients entiers de $x, u_1, \ldots, u_m$ qui devient identiquement congrue à o suivant $\mathfrak{p}^2$ pour $x = \xi$, Φ est divisible suivant p par Π^e.

Démonstration. — Posons $\Phi \equiv \Pi^{e'} F$ suivant $\mathfrak{p}$ où $e' < e$ et F une fonction à coefficients entiers de $x, u_1, u_2, \ldots, u_m$ qui n'est plus divisible par Π suivant p; il en résulte que tous les coefficients des puissances et produits de $u_1, \ldots, u_m$ dans

$$\{\Pi(\xi; u_1, \ldots, u_m)\}^{e'} F(\xi; u_1, \ldots, u_m$$

sont divisibles par $\mathfrak{p}^e$. Ordonnons $\Pi(\xi; u_1, \ldots, u_m)$ $F(\xi; u_1, \ldots, u_m)$ par rapport aux puissances décroissantes de u_1 et les coefficients des puissances de u_1 par rapport aux puissances décroissantes de u_2 et ainsi de suite. Soit π le premier coefficient dans Π qui n'est pas divisible par $\mathfrak{p}^2$ et en même temps par $\varkappa$ le premier coefficient de F qui n'est pas divisible par $\mathfrak{p}$, on aurait $\pi^{e'}\varkappa \equiv$ o suivant $\mathfrak{p}^e$, ce qui n'est pas possible; c'est-à-dire que tous les coefficients de F sont divisibles par $\mathfrak{p}$, et il en résulte d'après le lemme précédent que $F(x; u_1, \ldots, u_m)$ est encore divisible par $\Pi(x; u_1, \ldots, u_m)$ suivant $\mathfrak{p}$. Ce qui est contraire à l'hypothèse.

§ 11. — La décomposition du premier membre de l'équation fondamentale. Le discriminant de l'équation fondamentale.

Des lemmes 3, 4 et 5, nous tirerons :

THÉORÈME 33. — Si p décomposé en idéaux premiers donne $p = \mathfrak{p}^e \mathfrak{p}'^{e'} \ldots$, on a, pour le premier nombre de l'équation fondamentale au sens de la congruence suivant p,

$$F \equiv \Pi^e \Pi'^{e'} \ldots \qquad (p)$$

où Π, Π' représentent certaines fonctions irréductibles suivant p de x; $u_1, u_2, \ldots, u_m$; de plus, on peut poser

$$F = \Pi^e \Pi'^{e'} \ldots + pG$$

où G est une fonction entière à coefficients entiers contenant les variables x; $u_1, u_2, \ldots, u_m$, et qui n'est divisible suivant p par aucune des fonctions irréductibles Π, Π' ...

Théorème 34. — La congruence de degré m résultant de l'équation fondamentale

$$F(x; u_1, \ldots, u_m) \equiv 0 \qquad (p)$$

est la congruence de degré le moins élevée suivant p à laquelle satisfait la forme fondamentale ξ mise à la place de x.

Démonstration. — Soit Φ une fonction entière à coefficients entiers de x, u_1, u_2, ..., u_m telle que ξ satisfasse à $\Phi(x) \equiv 0$ suivant p, ξ étant la forme fondamentale. De plus, soient $\mathfrak{p}$, $\mathfrak{p}'$ ... les idéaux qui divisent p de degrés respectifs f, f' ... Si l'on forme la norme, on a $p^m = p^{fe+f'e'+\cdots}$, c'est-à-dire $m = fe + f'e' + \ldots$

De plus, soient Π, Π' ... les fonctions irréductibles relatives aux idéaux $\mathfrak{p}$, $\mathfrak{p}'$ ... qui ont été employées dans les lemmes précédentes. Du lemme (5) nous pouvons conclure que

$$\Phi \equiv \Pi^e \Pi'^{e'} \ldots \Psi \qquad (p)$$

où Ψ est une fonction entière. Comme Π, Π' sont de degrés f, f' ... en x, il en résulte que Φ est au moins de degré m, et cette circonstance nous donne, en prenant pour Φ le premier membre F de l'équation fondamentale, la première partie du théorème 33 et le théorème 34.

Si enfin $G(x)$ était divisible par $\Pi(x)$ suivant p, ξ mis à la place de x satisferait à $G(x) \equiv 0$ ($\mathfrak{p}$) et par suite ξ satisferait à la congruence $\Pi^e(x)\,\Pi'^{e'}(x) \ldots \equiv 0$ suivant $\mathfrak{p}^{e+1}$, ce qui n'est pas possible d'après le lemme (5), ce qui démontre la deuxième partie du théorème 33.

Les faits que nous venons d'établir entraînent une suite d'importants théorèmes relatifs aux discriminants.

Théorème 35. — Le plus grand facteur numérique du discriminant de l'équation fondamentale est égal au discriminant du corps.

Démonstration. — Posons

$$(2)\quad \begin{cases} 1 = U_{11}\,\omega_1 + \ldots + U_{1m}\,\omega_m, \\ \xi = U_{21}\,\omega_1 + \ldots + U_{2m}\,\omega_m, \\ \ldots\ldots\ldots\ldots\ldots \\ \xi^{m-1} = U_{m1}\,\omega_1 + \ldots + U_{mm}\,\omega_m, \end{cases}$$

où les U_{ik} sont des fonctions entières à coefficients entiers de $u_1, \ldots, u_m$. Si le déterminant U de ces m^2 fonctions était une fonction dont tous les coefficients sont divisibles par p (nombre premier), il existerait $V_1, \ldots, V_m$ fonctions entières à coefficients entiers de $u_1, \ldots, u_m$ non congrues entre elles suivant p et telles que l'on ait identiquement en $u_1, \ldots, u_m$:

$$V_1 U_{11} + \ldots + V_m U_{m1} \equiv 0, \qquad (p)$$
$$\ldots\ldots\ldots\ldots$$
$$V_1 U_{1m} + \ldots + V_m U_{mm} \equiv 0; \qquad (p)$$

par suite, la forme fondamentale ξ satisferait à la congruence

$$V_1 + V_2 \xi + \ldots + V_m \xi^{m-1} \equiv 0 \qquad (p)$$

qui est de degré inférieur à m, ce qui est impossible d'après le théorème (34).

Il en résulte que U est une forme rationnelle unité. Les équations (2) et le théorème relatif à la multiplication des déterminants nous donnent

$$\begin{vmatrix} 1, & \xi, & \ldots, & \xi^{m-1} \\ 1, & \xi', & \ldots, & \xi'^{m-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1, & \xi^{(m-1)}, & \ldots, & (\xi^{(m-1)})^{m-1} \end{vmatrix} = U \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega'_1, & \ldots, & \omega'_m \\ \ldots & \ldots & \ldots \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}.$$

En élevant au carré $d(\xi) = U^2 d$, $d(\xi) \simeq d$ où $d(\xi)$ désigne le discriminant de l'équation fondamentale et d le discriminant du corps.

En résolvant les équations (2) on a le résultat suivant :

Théorème 36. — Tout nombre entier du corps k est égal à une fonction rationnelle entière de degré $m - 1$ de la forme fondamentale ξ et les coefficients de cette fonction sont des fonctions entières à coefficients entiers des $u_1, \ldots, u_m$ divisées par la forme unité U. [Kronecker[16], Hensel[4].]

§ 12. — Les éléments et la différente du corps. — Démonstration du théorème relatif aux diviseurs du discriminant du corps.

Le théorème 35 permet la décomposition du discriminant d du corps en certains facteurs idéaux. Les $m - 1$ idéaux

$$\mathfrak{e}' = \left((\omega_1 - \omega'_1), \ \ldots, \ (\omega_m - \omega'_m)\right),$$
$$\mathfrak{e}'' = \left((\omega_1 - \omega''_1), \ \ldots, \ (\omega_m - \omega''_m)\right),$$
$$\ldots\ldots\ldots\ldots$$
$$\mathfrak{e}^{(m-1)} = \left((\omega_1 - \omega_1^{(m-1)}), \ \ldots, \ (\omega_m - \omega_m^{(m-1)})\right)$$

seront dits les $m-1$ *éléments* du corps k. Ce sont des idéaux qui, en général, ne font pas partie du corps k; mais le produit $\mathfrak{d} = \mathfrak{e}'\mathfrak{e}'' \ldots \mathfrak{e}^{(m-1)}$ est un idéal du corps k.

On expliquera plus loin comment certains idéaux d'un corps k peuvent être conçus aussi comme idéaux d'un corps plus élevé, car, si nous considérons que les éléments $\mathfrak{e}' \ldots, \mathfrak{e}^{(m-1)}$ sont les contenus des formes $\xi - \xi', \ldots, \xi - \xi^{(m-1)}$, nous reconnaissons, d'après le théorème 13, que l'idéal $\mathfrak{d}$ est le contenu de la différente de la forme fondamentale, c'est-à-dire de

$$\frac{\partial F}{\partial \xi} = (\xi - \xi') \ldots (\xi - \xi^{(m-1)})$$

qui est, elle, une forme du corps k. Nous dirons que $\mathfrak{d}$ est la *différente du corps* [1]. La norme de cet ideal est égal au plus grand facteur numérique du discriminant de la forme fondamentale, et, comme ce dernier est égal à d, on en conclut le théorème.

Théorème 37. — La norme de la différente d'un corps est égale au discriminant du corps.

De la congruence

$$\frac{\partial F(x)}{\partial x} \equiv e\Pi^{e-1} \frac{\partial \Pi}{\partial x} \Pi'^{e'} \ldots + e'\Pi^{e}\Pi'^{e'-1} \frac{\partial \Pi'}{\partial x} \ldots + \ldots \qquad (p)$$

il résulte de plus que la différente est toujours divisible par $\mathfrak{p}^{e-1}$ et qu'elle ne contient pas de puissance plus élevée de $\mathfrak{p}$, dès que l'exposant e est premier avec p. En passant à la norme, on voit que le discriminant d'un corps est toujours divisible par $p^{f(e-1)+f'(e'-1)+\ldots}$, et que de plus il ne contient pas p à une puissance plus élevée, si tous les exposants $e, e', \ldots$ sont premiers avec p; ceci démontre le théorème fondamental annoncé dès le début du paragraphe 10.

§ 13. — La formation des idéaux premiers. — Le diviseur numérique entier de la forme unité U_x.

Le calcul effectif des idéaux premiers qui divisent un nombre premier rationnel p peut être effectué d'après le paragraphe 33 en décomposant le premier nombre de l'équation fondamentale. Il est bon cependant de savoir dans quelles circonstances il est permis de donner aux paramètres $u_1, u_2, \ldots, u_m$ des valeurs particulières. C'est dans ce but que nous ferons les considérations suivantes.

On obtient les discriminants de tous les nombres entiers du corps en donnant dans U_d à $u_1, \ldots, u_m$ toutes les valeurs entières et rationnelles. Il n'est pas nécessaire

(1) D'après Dedekind, *L'idéal fondamental* « das Grundideal ».

que le plus grand commun diviseur de ces discriminants soit d, car il peut très bien se présenter le cas où la forme unité prend pour tous les nombres entiers de $u_1, \ldots, u_m$ une suite de valeurs ayant un diviseur entier $\gtrless 1$. C'est cela qui met en pleine lumière l'usage des indéterminées $u_1, \ldots, u_m$.

On trouve facilement une condition nécessaire et suffisante pour que le nombre premier rationnel p soit un diviseur entier de U; cette condition consiste en ce que U peut se mettre sous la forme

$$pV + (u_1^p - u_1)V_1 + \ldots + (u_m^p - u_m)V_m$$

où V, V_1, V_m sont des fonctions entières à coefficients entiers de $u_1, \ldots, u_m$. [Hensel [1, 2, 3].]

Si donc il est possible de donner aux indéterminées u_1, u_m des valeurs numériques entières rationnelles $a, a_1, \ldots, a_m$ telles que la forme unité devienne un nombre non divisible par p, lorsqu'on voudra décomposer p on pourra particulariser l'équation fondamentale en ce sens que la forme ξ pourra être remplacée par $\alpha = a_1\omega_1 + \ldots + \alpha_m\omega_m \ldots$. Et, en effet, sous les hypothèses que l'on a faites, et comme cela résulte du théorème 36, tout nombre entier ω du corps est congru à une certaine fonction de α suivant p, et c'est pourquoi une fonction entière à coefficients entiers de degré inférieur à m en α n'est jamais divisible par p si tous ses coefficients ne le sont. Désignons les fonctions de la seule variable x résultant des fonctions $\Pi(x; u_1, \ldots, u_m)$, $\Pi'(x; u_1, \ldots, u_m)$, ... par la substitution $u_1 = a_1, \ldots, u_m = a_m$; désignons-les par $P(x)$, $P'(x)$, ..., nous reconnaîtrons que ces fonctions, au sens de la congruence d'après p, sont des fonctions premières différentes les unes des autres et que

$$\mathfrak{p} = \big(p, P(\alpha)\big), \qquad \mathfrak{p}' = \big(p, P'(\alpha)\big), \qquad \ldots .$$

Et, en effet, si après avoir enlevé le facteur $\mathfrak{p}$, $P(\alpha)$ contenait encore un facteur contenu dans p soit $\mathfrak{p}'$, on aurait

$$\{P(\alpha)\}^{e}\{P'(\alpha)\}^{e'-1}\{P''(\alpha)\}^{e''}\ldots \qquad (p)$$

ce qui, d'après la remarque précédente, n'est pas possible, car nous avons là une congruence de degré inférieur à m en α.

Réciproquement on a le fait suivant : Si dans un corps on a $p = \mathfrak{p}^e\mathfrak{p}'^{e'} \ldots$ où $\mathfrak{p}, \mathfrak{p}' \ldots$ sont des idéaux premiers différents de degrés $f, f', \ldots$ et si à chacun de ces idéaux on peut faire correspondre une fonction entière à coefficients entiers $P(x)$, $P'(x)$, ... de la seule variable x de degrés $f, f', \ldots$ irréductibles suivant p et toutes différentes, on peut toujours trouver un nombre $\alpha = a_1\omega_1 + \ldots + a_m\omega_m$ tel que la valeur de U correspondante ne soit pas divisible par p.

La non-existence de fonctions premières $P(x)$, $P'(x)$, ... dans le sens de la congruence suivant le nombre rationnel p, forme donc une nouvelle condition nécessaire et suffisante pour que p soit diviseur entier de U. [Dedekind [4].]

Chacune des deux conditions trouvées dans ce paragraphe, et qui sont essentiellement différentes, peut servir au calcul d'exemples numériques pour des corps algébriques, dans laquelle les U contiennent des facteurs numériques entiers ± 1 et répondant à la question. [Dedekind[4], Kronecker[16], Hensel[1, 2, 5].]

Il faut cependant remarquer que la forme U perd la propriété de contenir des diviseurs entiers, si l'on y fait prendre à $u_1, \ldots, u_m$ les valeurs des nombres algébriques entiers d'un corps choisis de telle sorte que tous les nombres ainsi représentés par U aient pour plus grand commun diviseur 1.

CHAPITRE V.

Le corps relatif.

§ 14. — La norme relative, la différente relative et le discriminant relatif.

Les concepts de norme, de différente et de discriminant sont susceptibles d'une généralisation importante.

Si K est un corps de degré M, qui contient tous les nombres du corps k de degré m, k est dit un *sous corps* de K. Le corps K est dit le *sur-corps* ou le *corps relatif* par rapport à k. Soit Θ un nombre déterminant K. Parmi les équations en nombre infini à coefficients algébriques situés dans k auxquelles satisfait Θ, soit l'équation de degré r

$$(3) \qquad \Theta^r + \alpha_1 \Theta^{r-1} + \ldots + \alpha_r = 0$$

celle de degré le moins élevé; $\alpha_1, \ldots, \alpha_r$ sont alors des nombres déterminés de k; r s'appelle le *degré relatif* du corps K par rapport à k, et on a $M = rm$. L'équation (3) est irréductible dans le domaine de rationalité k. Si $\Theta', \ldots, \Theta^{(r-1)}$ sont les $r-1$ autres racines de l'équation (3), on dit que les $r-1$ nombres algébriques sont les nombres *relativement conjugués à* Θ, et les corps déterminés par $\Theta', \ldots, \Theta^{(r-1)}$, $K'K'', \ldots, K^{(r-1)}$ sont dits les corps *relativement conjugués à* K. Soit A un nombre quelconque du corps K et

$$A = \gamma_1 + \gamma_2 \Theta + \ldots + \gamma_r \Theta^{r-1}$$

où $\gamma_1, \gamma_2, \ldots, \gamma_r$ sont des nombres dans k, les nombres

$$A' = \gamma_1 + \gamma_2 \Theta' + \ldots + \gamma_r \Theta'^{r-1},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$A^{(r-1)} = \gamma_1 + \gamma_2 \Theta^{(r-1)} + \ldots \gamma_r (\Theta^{(r-1)})^{r-1}$$

sont dits issus de A par les substitutions $T' = (\Theta : \Theta'), \dots, T^{(r-1)} = (\Theta : \Theta^{(r-1)})$, ou encore les nombres *relativement conjugués à* A. Si l'on applique la substitution T' à tous les nombres d'un idéal $\mathfrak{J}$, on obtient un idéal $\mathfrak{J}'$ qui est l'idéal issu de $\mathfrak{J}$ par la substitution T' ou l'idéal relativement conjugué à $\mathfrak{J}$.

Soient $\alpha_1, \dots, \alpha_s$ des nombres quelconques dans k et soit $\mathfrak{j} = (\alpha_1, \dots, \alpha_s)$ l'idéal que ces nombres déterminent dans k, ces mêmes nombres déterminent un idéal $\mathfrak{J} = (\alpha_1, \dots, \alpha_s)$ dans K. Cet idéal $\mathfrak{J}$ ne doit pas être considéré comme différent de $\mathfrak{j}$.

Le théorème qui va suivre nous permet de considérer $(\alpha_1, \dots, \alpha_s)$ à la fois comme un idéal dans k et dans K.

Si $\alpha_1, \alpha_2, \dots, \alpha_s$ et $\alpha_1^0, \dots, \alpha_s^0$ sont des entiers dans k tels que dans K les idéaux $\mathfrak{J} = (\alpha_1, \dots, \alpha_s)$, $\mathfrak{J}^0 = (\alpha_1^0, \dots, \alpha_s^0)$ coïncident, dans k les deux idéaux $\mathfrak{j} = (\alpha_1, \dots, \alpha_s)$, $\mathfrak{j}_0 = (\alpha_1^0, \dots, \alpha_s^0)$ coïncident aussi. En effet, par suite de l'hypothèse, si α^0 est un des nombres $\alpha_1^0, \dots, \alpha_s^0$, on a $\alpha^0 = A_1\alpha_1 + \dots + A_s\alpha_s$, où $A_1, \dots, A_s$ sont certains nombres entiers dans K. Si nous formons la norme relative de chacune de ces deux expressions, nous reconnaissons que, dans k, $\alpha^{0'}$ doit être divisible par $\mathfrak{j}'$; par suite, dans k, α^0 est divisible par $\mathfrak{j}$ et par suite aussi $\mathfrak{j}^0$ est divisible par $\mathfrak{j}$. Comme, d'autre part, on peut démontrer la réciproque, il faut que dans ce cas $\mathfrak{j} = \mathfrak{j}^0$.

Au contraire, un idéal $\mathfrak{J} = (A_1, \dots, A_s)$ du corps K ne sera un idéal $\mathfrak{j}$ du corps k que si $\mathfrak{J}$ est diviseur commun de certains nombres $\alpha_1, \dots, \alpha_s$ du corps k.

Le produit d'un nombre A par tous ses conjugués relatifs

$$N_k(A) = AA' \dots A^{(r-1)}$$

est dit la *norme relative du nombre* A par rapport au corps k ou dans le domaine de rationalité k. La norme relative N_k est un nombre de k.

Soit $\mathfrak{J} = (A_1, \dots, A_s)$ un idéal quelconque dans K, le produit de $\mathfrak{J}$ par tous les idéaux relativement conjugués

$$N_k(\mathfrak{J}) = \mathfrak{J}\mathfrak{J}' \dots \mathfrak{J}^{(r-1)}$$

est la *norme relative de* $\mathfrak{J}$. La norme relative $N_k(\mathfrak{J})$ est un idéal du corps k. Car si $U_1, \dots, U_S$ désignent des indéterminées, les coefficients du produit

$$(A_1U_1 + \dots + A_SU_S)(A'_1U_1 + \dots + A'_SU_S) \dots (A_1^{(r-1)}U_1 + \dots + A_S^{(r-1)}U_S)$$

sont des nombres entiers dans k, dont le plus grand diviseur coïncide avec ce produit d'idéaux d'après le théorème 13.

L'expression

$$\Delta_k(A) = (A - A')(A - A'') \dots (A - A^{(r-1)})$$

représente un nombre du corps K et se nomme la *différente relative du nombre* A par rapport à k. L'expression

$$D_k(A) = (A - A')^2(A - A'')^2 \dots (A^{(r-2)} - A^{(r-1)})^2$$

est de *discriminant relatif du nombre* A. Ce discriminant est égal au signe près, à la norme relative de la différente relative de A; car on a

$$D_k(A) = (-1)^{\frac{r(r-1)}{2}} N_k(\Delta_k).$$

Si $\Omega_1, \ldots, \Omega_M$ sont les M nombres de la base du corps K, l'idéal que l'on obtient en faisant le produit des $r-1$ éléments

$$\mathfrak{E}' = \big((\Omega_1 - \Omega_1'), \quad \ldots, (\Omega_M - \Omega_M')\big),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\mathfrak{E}^{(r-1)} = \big((\Omega_1 - \Omega_1^{(r-1)}), \ldots, (\Omega_M - \Omega_M^{(r-1)})\big),$$

c'est-à-dire

$$\mathfrak{D}_k = \mathfrak{E}'\mathfrak{E}'' \ldots \mathfrak{E}^{(r-1)},$$

est la *différente relative du corps* K par rapport à k.

Si l'on désigne par

$$\Xi = \Omega_1 U_1 + \ldots + \Omega_M U_M$$

la forme fondamentale de K, la différente relative de Ξ est

$$\Delta_k(\Xi) = (\Xi - \Xi') \ldots (\Xi - \Xi^{(r-1)}).$$

Les coefficients de cette forme sont des nombres du corps K, et comme d'après le théorème 13 leur plus grand commun diviseur est la différente relative $\mathfrak{D}_k$, $\mathfrak{D}_k$ est un idéal du corps K.

Le carré du plus grand commun diviseur de tous les déterminants à r lignes de la matrice

$$(4)\qquad \begin{vmatrix} \Omega_1, & \Omega_2, & \ldots, & \Omega_M \\ \Omega_1', & \Omega_2', & \ldots, & \Omega_M' \\ \cdots & \cdots & \cdots & \cdots \\ \Omega_1^{(r-1)}, & \Omega_2^{(r-1)}, & \ldots, & \Omega_M^{(r-1)} \end{vmatrix}$$

s'appelle le *discriminant relatif* D_k du corps K relatif à k; ce discriminant, on le voit facilement, est un idéal du corps k.

§ 15. — Propriétés de la différente relative et du discriminant relatif d'un corps.

Pour les concepts que l'on vient de définir, on a les théorèmes suivants [Hilbert[3]] :

Théorème 38. — Le discriminant relatif du corps K par rapport au sous-corps k est égal à la norme relative de la différente relative de K, c'est-à-dire

$$D_k = N_k(\mathfrak{D}_k).$$

Démonstration. — La norme relative de la différente relative de la forme fondamentale Ξ est

$$N_k\big(\Delta_k(\Xi)\big) = \pm(\Xi - \Xi')^2(\Xi - \Xi'')^2 \ldots (\Xi^{(r-2)} - \Xi^{(r-1)})^2$$

$$= \pm \begin{vmatrix} 1, & \Xi, & \ldots, & \Xi^{r-1} \\ 1, & \Xi', & \ldots, & (\Xi')^{r-1} \\ \cdot & \cdot & \cdot & \cdot \\ 1, & \Xi^{(r-1)}, & \ldots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix}^2.$$

D'autre part, le carré du déterminant est une forme du corps K dont le contenu est égal au discriminant relatif D_k. Car si nous exprimons les termes de ce déterminant en fonction linéaire de $\Omega_1, \ldots, \Omega_M$ et de leurs conjugués dans le corps K, où les coefficients de ces expressions sont des fonctions entières à coefficients entiers de $U_1, \ldots, U_M$, nous reconnaîtrons que le carré de ce déterminant n'a que des coefficients divisibles par D_k.

Réciproquement, une généralisation du théorème 36 nous montre que chaque déterminant à r lignes de la matrice (4) multipliée par la $r^{\text{ème}}$ puissance d'une certaine forme unitaire rationnelle des paramètres $U_1, \ldots, U_M$ est divisible par le produit

$$(\Xi - \Xi')(\Xi - \Xi'') \ldots (\Xi^{(r-2)} - \Xi^{(r-1)}).$$

Il en résulte que $N_k\big(\Delta_k(\Xi)\big) \simeq D_k$.

THÉORÈME 39. — Si D et d désignent le discriminant du sur-corps K et du sous-corps k, et si l'on désigne par $n(D_k)$ la norme du discriminant relatif D_k pris dans le corps k, on a

$$D = d^r n(D_k).$$

Démonstration. — Si $\xi = \omega_1 u_1 + \ldots + \omega_m u_m$ est la forme fondamentale du corps k, Ξ mis à la place de X satisfait à une équation de degré r en X de la forme

$$\Phi(X, \xi) = \Phi_0 X^r + \Phi_1 X^{r-1} + \ldots + \Phi_r = 0$$

où $\Phi_1, \ldots, \Phi_r$ sont des fonctions entières à coefficients entiers de ξ et des indéterminées $u_1, \ldots, u_m, U_1, \ldots, U_M$, et où Φ_0 est une forme unitaire rationnelle des indéterminées $u_1, \ldots, u_m$. Les autres racines de l'équation de degré dont nous venons de parler sont $X = \Xi', \ldots, \Xi^{(r-1)}$. Soit donc $\xi^{(h)}$ une des $m - 1$ formes fondamentales conjuguées à ξ, et soient $\Xi_{(h)}, \Xi'_{(h)}, \ldots, \Xi_{(h)}^{(r-1)}$ les racines de l'équation de degré r, $\Phi(X, \xi^{(h)}) = 0$. Comme ξ satisfait à une équation de degré M, il est évident que toute puissance de Ξ multipliée par une puissance de Φ_0 est égale à une fonction entière de ξ et de Ξ, qui est au plus de degré $m - 1$ en ξ et au plus de degré $r - 1$ en Ξ et dont les coefficients sont des fonctions entières à coefficients entiers des paramètres

$u_1, \dots, u_m, U_1, \dots, U_M$. D'après cela, le discriminant de la forme fondamentale Ξ, multiplié par une puissance de Φ_0, est divisible par le carré du déterminant à $M = rm$ lignes.

$$\Delta = \begin{vmatrix} 1, \Xi, & \dots, \Xi^{r-1}, & \xi, \xi\Xi, & \dots, \xi\Xi^{r-1}, & \dots, \xi^{m-1}, \xi^{m-1}\Xi, & \dots, \xi^{m-1}\Xi^{r-1} \\ 1, \Xi', & \dots, \Xi'^{r-1}, & \xi, \xi\Xi', & \dots, \xi\Xi'^{r-1}, & \dots, \xi^{m-1}, \xi^{m-1}\Xi', & \dots, \xi^{m-1}\Xi'^{r-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1, \Xi^{r-1}, & \dots, (\Xi^{(r-1)}), & \xi, \xi\Xi^{(r-1)}, & \dots, \xi(\Xi^{(r-1)})^{r-1}, & \dots, \xi^{m-1}, \xi^{m-1}\Xi^{r-1}, & \dots, \xi^{m-1}(\Xi^{(r-1)})^{r-1} \end{vmatrix}$$

Dans ce schéma, nous n'avons écrit que les r premières lignes horizontales ; on obtiendra les $(m-1)r$ autres en donnant successivement aux lettres ξ le signe $(h) = (1), \dots, (m-1)$ comme indices supérieurs et à toutes les lettres Ξ les mêmes signes comme indices inférieurs.

Si l'on exprime les éléments du déterminant Δ en fonction linéaire des nombres de la base, on reconnaît l'exactitude de la formule

$$\Delta = \begin{vmatrix} \Omega_1, & \dots, & \Omega_M \\ \Omega'_1, & \dots, & \Omega'_M \\ \dots & \dots & \dots \\ \Omega_1^{(M-1)}, & \dots, & \Omega_M^{(M-1)} \end{vmatrix} F,$$

où F est une fonction entière à coefficients entiers des paramètres $u_1, \dots, u_m, U_1, \dots, U_m$. Mais comme le facteur numérique du discriminant de Ξ d'après le théorème $35 = D$, il résulte du développement précédent que réciproquement D est divisible par le facteur numérique du carré de Δ, c'est-à-dire que le facteur numérique de Δ^2 est égal à D.

Par les théorèmes élémentaires de la théorie des déterminantes, on obtient l'identité

$$\Delta = \begin{vmatrix} 1, & \xi, & \dots, & \xi^{m-1} \\ 1, & \xi', & \dots, & \xi'^{m-1} \\ \dots & \dots & \dots & \dots \\ 1, & \xi^{(m-1)}, & \dots, & (\xi^{(m-1)})^{m-1} \end{vmatrix}^r \Pi,$$

$$\Pi = \begin{vmatrix} 1, & \Xi, & \dots, & \Xi^{r-1} \\ 1, & \Xi', & \dots, & \Xi'^{r-1} \\ \dots & \dots & \dots & \dots \\ 1, & \Xi^{(r-1)}, & \dots, & (\Xi^{(r-1)})^{r-1} \end{vmatrix} \begin{vmatrix} 1, & \Xi_{(1)}, & \dots, & \Xi_{(1)}^{r-1} \\ 1, & \Xi'_{(1)}, & \dots, & \Xi'^{r-1}_{(1)} \\ \dots & \dots & \dots & \dots \\ 1, & \Xi^{(r-1)}_{(1)}, & \dots, & (\Xi^{(r-1)}_{(1)})^{r-1} \end{vmatrix} \cdots \begin{vmatrix} 1, & \Xi^{(r-1)}_{(m-1)}, & \dots, & (\Xi^{(r-1)}_{(m-1)})^{r-1} \\ 1, & \Xi_{(m-1)}, & \dots, & \Xi^{(r-1)}_{(m-1)} \\ \dots & \dots & \dots & \dots \\ 1, & \Xi'_{(m-1)}, & \dots, & (\Xi'^{(r-1)}_{(m-1)})^{r-1} \end{vmatrix},$$

ce qui donne immédiatement le théorème 39.

Le théorème démontré à l'instant ne montre pas seulement que le déterminant d'un corps est divisible par le discriminant de tout sous-corps, mais il indique la puissance de ce dernier qui est contenue dans le discriminant du sur-corps, et il donne la signification simple du facteur restant dans le déterminant du sur-corps.

§ 16. — La décomposition d'un élément du corps k dans le sur-corps K. Le théorème sur la différente du sur-corps K.

Théorème 40. — Tout élément du sous-corps k est égal à un produit de r certains éléments du sur-corps K, et on a les formules

$$\xi - \xi^{(h)} \simeq (\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \dots (\Xi - \Xi_{(h)}^{(r-1)}) \simeq (\Xi - \Xi_{(h)})(\Xi' - \Xi_{(h)}) \dots (\Xi^{(r-1)} - \Xi_{(h)}).$$

Démonstration. — Soit

$$F(X) = X^M + F_1 X^{M-1} + \dots + F_M = 0$$

l'équation fondamentale de degré M du corps K, où $F_1, \dots, F_M$ sont des fonctions entières à coefficients entiers des $U_1, \dots, U_M$, on a identiquement

$$\Phi_0^m F(X) = \Phi(X, \xi)\Phi(X, \xi') \dots \Phi(X, \xi^{(m-1)}).$$

La différente de la forme fondamentale Ξ est donc représentée par la formule

$$\Delta(\Xi) = \frac{\partial F(\Xi)}{\partial \Xi} = \frac{1}{\Phi_0^m} \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi} \Phi(\Xi, \xi') \dots \Phi(\Xi, \xi^{(m-1)})$$

en vertu de $\Phi(\Xi, \xi) = 0$.

Mais on a d'une part

(5) $$\Phi(\Xi, \xi^{(h)}) = \Phi_0(\Xi - \Xi_{(h)})(\Xi - \Xi'_{(h)}) \dots (\Xi - \Xi_{(h)}^{(r-1)}),$$
$$(h = 1, 2, \dots, m-1)$$

et d'autre part

(6) $$\Phi(\Xi, \xi^{(h)}) = \Phi(\Xi, \xi^{(h)}) - \Phi(\Xi, \xi) = (\xi - \xi^{(h)}) G^{(h)}$$

où $G^{(h)}$ représente une forme algébrique entière ; il résulte de ces formules que

$$\Phi_0^m \frac{\partial F(\Xi)}{\partial \Xi} = \frac{\partial \Phi(\Xi, \xi)}{\partial \Xi} (\xi - \xi') \dots (\xi - \xi^{(m-1)}) G' \dots G^{(m-1)}.$$

Comme $\dfrac{1}{\Phi_0} \dfrac{\partial \Phi(\Xi, \xi)}{\partial \Xi}$ représente la différente relative de Ξ, il résulte, d'après le théorème 13 de la dernière formule, que

(7) $$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d} \mathfrak{J}$$

où $\mathfrak{D}$ est la différente de k, $\mathfrak{D}_k$ la différente relative de K par rapport à k, et où $\mathfrak{J}$ représente l'idéal égal au contenu de la forme $G', \dots, G^{(m-1)}$.

En passant aux normes

$$D = n(D_k)\, d\, N(\mathfrak{J})$$

et, par suite, d'après le théorème 39, $N(\mathfrak{J}) = 1$, c'est-à-dire $\mathfrak{J} = 1$. Les formes $G_1, \dots, G^{(m-1)}$ sont donc toutes des formes unités, et les formules (5) et (6) démontrent notre théorème 40.

Le théorème 40 donne la décomposition des éléments du corps k dans le *surcorps* K; il est le théorème fondamental de la théorie des discriminants.

La formule (7) nous fournit de plus l'important fait suivant :

Théorème 41. — La différente $\mathfrak{D}$ du corps K est égale au produit de la différente relative $\mathfrak{D}_k$ de K par rapport au sous-corps k et la différente $\mathfrak{d}$ du corps k, c'est-à-dire

$$\mathfrak{D} = \mathfrak{D}_k \mathfrak{d}.$$

On voit quel rapport simple existe entre les différentes.

La différente du corps supérieur s'obtient en multipliant la différente du corps inférieur par la différente relative correspondante.

CHAPITRE VI.

Les unités du corps.

§ 17. — De l'existence des nombres conjugués, dont les valeurs absolues satisfont a certaines inégalités.

Nous avons établi au chapitre II les lois de la divisibilité des nombres d'un corps algébrique, nous allons établir maintenant des vérités fondées avant tout sur l'idée de grandeur. C'est le théorème de [Minkowski[3]] qui va nous fournir le moyen le plus puissant dans ces recherches ; il s'énonce ainsi :

Lemme 6. — Soit

$$f_1 = a_{11} u_1 + \dots + a_{1m} u_m,$$
$$\dots\dots\dots\dots\dots$$
$$f_m = a_{m1} u_1 + \dots + a_{mm} u_m$$

m formes linéaires et homogènes de $u_1, \dots, u_m$ à coefficients réels quelconques et de déterminant égal à 1 ; on peut déterminer pour $u_1, u_2, \dots, u_m$ des valeurs entières et rationnelles qui ne sont pas toutes nulles telles que les m formes $f_1, \dots, f_m$ soient toutes en valeur absolue $\leqq 1$.

Ce théorème, légèrement transformé, nous donne :

Lemme 7. — Soient $f_1, f_2, \dots, f_m$ m formes linéaires et homogènes de $u_1, u_2, \dots, u_m$ à coefficients réels quelconques avec un déterminant positif Δ, et soient $\varkappa_1, \varkappa_2, \varkappa_3, \dots, \varkappa_m$ m constantes quelconques positives dont le produit est égal à Δ, on peut toujours

déterminer m valeurs entières et rationnelles pour $u_1, u_2, \ldots, u_m$ qui ne sont pas toutes nulles et telles que

$$|f_1| \leqq \varkappa_1, \quad \ldots, \quad |f_m| \leqq \varkappa_m.$$

Dans ce chapitre, nous désignerons le corps k et les $m-1$ conjuguées par $k = k^{(1)}, k^{(2)}, \ldots, k^{(m)}$, et nous désignerons les m nombres de bases du corps $k^{(s)}$ par $\omega_1^{(s)}, \ldots, \omega_m^{(s)}$.

Nous appliquerons le lemme 7 pour démontrer le

THÉORÈME 42. — *Soient $\varkappa_1, \varkappa_2, \ldots, \varkappa_m$ m constantes positives quelconques dont le produit est égal à $\sqrt{d}$, et qui satisfont aux conditions $\varkappa_s = \varkappa_{s'}$ dans le cas où $k^{(s)}$ et $k^{(s')}$ sont deux corps imaginaires conjugués, il y a toujours dans le corps k un nombre entier différent de zéro ω tel que*

$$|\omega^{(1)}| \leqq \varkappa_1, \quad \ldots, \quad |\omega^{(m)}| \leqq \varkappa_m.$$

Démonstration. — Nous attribuerons aux corps $k^{(1)}, k^{(2)}, \ldots, k^{(m)}$ certaines formes linéaires, et nous nous placerons au point de vue suivant. Si $k^{(r)}$ est un corps réel, nous lui attribuerons la forme réelle

$$f_r = \omega_1^{(r)} u_1 + \ldots + \omega_m^{(r)} u_m;$$

si $k^{(s)}$ est un corps imaginaire et si $k^{(s')}$ est son imaginaire conjugué, nous attribuerons aux deux corps $k^{(s)}$ et $k^{(s')}$ les deux formes linéaires

$$(8)\qquad \begin{cases} f_{s'} = \dfrac{1}{\sqrt{2}} \{ (\omega_1^{(s)} + \omega_1^{(s')}) u_1 + \ldots + (\omega_m^{(s)} + \omega_m^{(s')}) u_m \}, \\[2ex] f_s = \dfrac{1}{i\sqrt{2}} \{ (\omega_1^{(s)} + \omega_1^{(s')}) u_1 + \ldots + (\omega_m^{(s)} + \omega_m^{(s')}) u_m \} \end{cases}$$

dont les coefficients sont réels. Le déterminant de ces m formes pris en valeur absolue $= |\sqrt{d}|$. Le lemme 7 apporte immédiatement la preuve de notre affirmation si l'on remarque que

$$f_s^2 + f_{s'}^2 = 2\,|\omega_1^{(s)} u_1 + \ldots + \omega_m^{(s)} u_m|^2.$$

Il résulte de là, en outre, le

THÉORÈME 43. — *Le degré m et la constante positive $\varkappa$ étant donnés, il n'y a qu'un nombre limité de nombres entiers algébriques de degré m, qui, avec leurs conjugués, sont tous $< \varkappa$ en valeur absolue.*

Démonstration. — Les m coefficients entiers de l'équation à laquelle satisfait un pareil nombre sont tous inférieurs à une limite qui ne dépend que de m et de $\varkappa$; leur nombre est donc limité.

§ 18. — Théorèmes relatifs a la valeur absolue du discriminant du corps.

Théorème 44. — Le discriminant d d'un corps k n'est jamais égal à ± 1. [Minkowski[1, 2, 3].]

Théorème 45. — Il n'y a qu'un nombre fini de corps de degré m et de discriminant donné d. [Hermite[1, 2], Minkowski[3].]

Nous démontrerons d'abord le

Lemme 8. — Soient $f_1, f_2, \ldots, f_m$ les m formes réelles linéaires définies par les formules (8) des variables $u_1, u_2, \ldots, u_m$, il y a toujours dans le corps un nombre entier différent de zéro $\alpha = a_1 \omega_1 + \ldots + a_m \omega_m$ tel que les valeurs absolues de ces formes pour $u_1 = a_1 \ldots u_m = a_m$ satisfassent aux conditions

$$(9) \qquad |f_1| \leqslant |\sqrt{d}|, \quad |f_2| < 1, \quad |f_3| < 1, \quad \ldots, \quad |f_m| < 1.$$

Démonstration. — D'après le théorème 43, il n'y a qu'un nombre fini de nombres $\alpha, \alpha_1, \alpha_2, \ldots$ du corps k satisfaisant à

$$|f_1| < |\sqrt{d}| + 1, \quad |f_2| < 1, \quad \ldots, \quad |f_m| < 1.$$

Soit α parmi ces nombres celui qui donne à $|f_1|$ la plus petite valeur et soit φ cette plus petite valeur. S'il n'existait pas de pareil nombre, on poserait $\varphi = |\sqrt{d}| + 1$. Si $\varphi \leqslant |\sqrt{d}|$ le théorème est évident. Dans le premier cas, nous déterminerons un nombre positif ε tel que $(1 + \varepsilon)^{m-1} |\sqrt{d}| < \varphi$. D'après le lemme 7, il y a toujours un système d'entiers rationnels $u_1, \ldots, u_m$ tels que

$$|f_1| \leqslant (1 + \varepsilon)^{m-1} |\sqrt{d}|, \quad |f_2| \leqslant \frac{1}{1 + \varepsilon}, \quad \ldots, \quad |f_m| \leqslant \frac{1}{1 + \varepsilon},$$

et par suite

$$|f_1| < \varphi, \quad |f_2| < 1, \quad \ldots, \quad |f_m| < 1,$$

ce qui est contraire à l'hypothèse qui nous a fait choisir α.

Pour démontrer dès lors les théorèmes 44 et 45, nous procéderons ainsi. Si $k = k^{(1)}$ est un corps réel, la forme f_1 est parfaitement déterminée; si $k^{(1)}$ est corps imaginaire et $k^{(2)}$ son corps imaginaire conjugué, nous pouvons choisir pour f_1 entre deux formes; nous prendrons

$$f_1 = \frac{1}{i\sqrt{2}} \{ (\omega_1^{(1)} - \omega_1^{(2)}) u_1 + \ldots + (\omega_m^{(1)} - \omega_m^{(2)}) u_m \}.$$

La suite dans laquelle nous adopterons les autres formes $f_2, \ldots, f_m$ n'importe pas. Le lemme 8 nous montre l'existence d'un nombre α satisfaisant aux conditions (9).

D'autre part,

$$\prod_{(r)} |f_r| \prod_{s,s'} \frac{f_s^2 + f_{s'}^2}{2} = |n(\alpha)|;$$

comme on a nécessairement $|n(\alpha)| \geqq 1$, il en résulte $|f_1| > 1$, et par suite $|\sqrt{d}| > 1$. Le théorème 44 est démontré.

Il résulte, d'autre part, des inégalités $|f_1| > 1$, $|f_2| < 1$, $|f_3| < 1$, $|f_m| < 1$, que α est un nombre du corps $k = k^{(1)}$ qui diffère de tous ses conjugués, c'est-à-dire que la différente $\delta(\alpha) \neq 0$. D'après une remarque faite précédemment, α est un nombre qui détermine le corps k.

D'autre part, comme d est un nombre donné, on voit, d'après le théorème 43, qu'il n'y a qu'un nombre limité de nombres entiers algébriques de degré m, qui, avec leurs conjugués, satisfont aux conditions (9), ce qui nous démontre immédiatement le théorème 45.

Le théorème 44 exprime une propriété essentielle des corps algébriques : il montre que le discriminant de tout corps contient au moins *un* nombre *premier*.

En employant au lieu du lemme 6 un théorème plus profond dû également à Minkowski, le même raisonnement nous aurait montré que le discriminant d'un corps de degré m dépasse certainement en valeur absolue $\left(\frac{\pi}{4}\right)^{2r_2}\left(\frac{m^m}{m!}\right)^2$ et à plus forte raison $\left(\frac{\pi}{4}\right)^{2r_2} \frac{e^{2m-\frac{1}{6m}}}{2\pi m}$ où r_2 désigne le nombre de couples de corps imaginaires qui se trouvent parmi $k^{(1)}, \ldots, k^{(m)}$. [Minkowski[1, 2, 3].]

Ce dernier fait, appliqué de la même manière, montre que parmi les corps de tous les degrés possibles il n'y en a qu'un nombre limité ayant un discriminant donné d.

De ces mêmes principes, nous tirerons encore une conséquence très importante pour le chapitre VII. [Minkowski[1, 3].]

THÉORÈME 46. — Soit $\mathfrak{a}$ un idéal donné du corps k, il y a toujours un nombre α du corps différent de o divisible par $\mathfrak{a}$ et tel que

$$|n(\alpha)| \leqq \left| n(\mathfrak{a})\sqrt{d} \right|.$$

Démonstration. — Soient

$$\iota_1 = a_{11}\omega_1 + \ldots + a_{1m}\omega_m,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$\iota_m = a_{m1}\omega_1 + \ldots + a_{mm}\omega_m$$

les m nombres de base de l'idéal $\mathfrak{a}$; formons comme nous l'avons fait précédemment, au moyen de $\omega_1, \ldots, \omega_m$, m formes linéaires $f_1, \ldots, f_m$ à coefficients réels ; la valeur du déterminant de ces m formes sera

$$\begin{vmatrix} \iota_1^{(1)}, & \ldots, & \iota_m^{(1)} \\ \ldots & \ldots & \ldots \\ \iota_1^{(m)}, & \ldots, & \iota_m^{(m)} \end{vmatrix} = \begin{vmatrix} a_{11}, & \ldots, & a_{1m} \\ \ldots & \ldots & \ldots \\ a_{m1}, & \ldots, & a_{mm} \end{vmatrix} \begin{vmatrix} \omega_1^{(1)}, & \ldots, & \omega_m^{(1)} \\ \ldots & \ldots & \ldots \\ \omega_1^{(m)}, & \ldots, & \omega_m^{(m)} \end{vmatrix}$$

qui, d'après le théorème 19, égale en valeur absolue $|n(\mathfrak{a})\sqrt{d}|$. Si maintenant nous attribuons aux m formes $f_1, f_2, \ldots, f_m$ l'une des constantes réelles $\varkappa_1, \varkappa_2, \ldots, \varkappa_m$ dont le produit $= |n(\mathfrak{a})\sqrt{d}|$ et qui satisfont aux conditions $\varkappa_s = \varkappa_{s'}$ dans le cas où $k^{(s)}$ et $k^{(s')}$ sont des corps imaginaires conjugués, le théorème 46 résulte du théorème 42.

§ 19. — Le théorème qui prouve l'existence des unités du corps. — Un théorème auxiliaire au sujet d'une unité possédant une propriété particulière.

Le théorème qui va suivre, relatif aux unités du corps k, nous donne la base fondamentale d'une étude plus approfondie des nombres entiers algébriques.

Mais tout d'abord nous appellerons *unité* du corps k tout nombre entier ε dont la valeur inverse $\frac{1}{\varepsilon}$ est encore un nombre entier. La norme d'une unité $= \pm 1$, et, réciproquement, si la norme d'un entier du corps $= \pm 1$, ce nombre est une unité du corps.

Théorème 47. — *Supposons que parmi les m corps conjugués $k^{(1)}, \ldots, k^{(m)}$ il y ait r_1 corps réels et $r_2 = \frac{m - r_1}{2}$ corps imaginaires conjugués, le corps $k = k^{(1)}$ contient un système de $r = r_1 + r_2 - 1$ unités $\varepsilon_1, \ldots, \varepsilon_r$ telles que toute autre unité du corps peut être mise sous la forme $\varepsilon = \rho\,\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}$ et cela d'une seule manière, $a_1, \ldots, a_r$ étant des nombres entiers rationnels et ρ une racine de l'unité située dans k.*

Pour préparer la démonstration de ce théorème, nous ordonnerons les m corps conjugués $k^{(1)}, \ldots, k^{(m)}$ de la façon suivante :

Nous écrirons d'abord les r_1 corps réels $k^{(1)} \ldots, k^{(r)}$, puis nous prendrons un corps de chaque couple de corps imaginaires conjugués $k^{(r_1+1)}, \ldots, k^{(r_1+r_2)}$, et nous ferons suivre ces derniers de leurs corps conjugués $k^{(r_1+r_2+1)}, \ldots, k^{(m)}$. Nous formerons, avec m variables réelles quelconques $u_1, u_2, \ldots, u_m$, les m formes linéaires

$$\xi_s = \omega_1^{(s)} u_1 + \ldots + \omega_m^{(s)} u_m, \qquad (s = 1, 2, \ldots, m)$$

et nous écrirons $\xi_1 = \xi$. Si $\xi_1, \ldots, \xi_m$ sont tous $\neq 0$, nous poserons, dans le cas de $k^{(s)}$ réel :

$$\log|\xi_s| = l_s(\xi),$$

et dans le cas où $k^{(s)}$ et $k^{(s')}$ sont des corps imaginaires conjugués :

$$\log(\xi_s) = \tfrac{1}{2} l_s(\xi) - i\,l_{s'}(\xi),$$
$$\log(\xi_{s'}) = \tfrac{1}{2} l_s(\xi) + i\,l_{s'}(\xi),$$

où $l_1(\xi), \ldots, l_m(\xi)$ sont tous des grandeurs réelles et où en particulier les formes $l_{s'}(\xi)$ satisfont à

$$0 \leqq l_{s'}(\xi) < 2\pi;$$

les grandeurs $l_1(\xi), \ldots, l_m(\xi)$ ont donc une détermination unique en fonction des variables réelles $u_1, u_2, \ldots, u_m$, nous les appellerons *logarithmes de la forme* ξ. De plus, si l'on désigne par $ln(\xi)$ la partie réelle du logarithme de $n(\xi)$, on a

$$l_1(\xi) + \ldots + l_{r+1}(\xi) = ln(\xi).$$

Si $u_1, \ldots, u_m$ sont des entiers rationnels qui ne sont pas tous nuls, $\xi = \xi_1$ représente un nombre $\alpha \neq 0$ du corps $k = k^{(1)}$. Les grandeurs $l_1(\xi), \ldots, l_m(\xi)$ sont alors parfaitement déterminées par α et nous les nommerons les *logarithmes du nombre* α.

Si ε est une unité du corps k, on a en vertu de $n(\varepsilon) = \pm 1$:

$$l_1(\varepsilon) + l_2(\varepsilon) + \ldots + l_{r+1}(\varepsilon) = 0.$$

Par contre, les logarithmes $l_1(\xi), \ldots, l_m(\xi)$ nous donnent pour les variables $u_1, u_2, \ldots, u_m$ 2^{r_1} valeurs, car les r_1 valeurs réelles $\xi_1, \xi_2, \ldots, \xi_{r_1}$ ne sont déterminées qu'au signe près, tandis que les valeurs imaginaires conjuguées $\xi_{r_1+1}, \ldots, \xi_m$ sont parfaitement déterminées.

Nous aurons à nous servir du déterminant fonctionnel de ces relations ; nous désignerons le déterminant fonctionnel des fonctions $f_1, f_2, \ldots, f_m$ des variables $x_1, x_2, \ldots, x_m$ par $\dfrac{f_1, \ldots, f_m}{x_1, \ldots, x_m}$.

On a entre les valeurs absolues les relations

$$\left|\frac{u_1, \ldots, u_m}{\xi_1, \ldots, \xi_m}\right| = \frac{1}{\sqrt{d}}; \qquad \left|\frac{\xi_1, \ldots, \xi_m}{l_1(\xi), \ldots, l_m(\xi)}\right| = |\xi_1 \ldots \xi_m| = |n(\xi)|,$$

et en multipliant ces deux relations nous aurons

$$\left|\frac{u_1, \ldots, u_m}{l_1(\xi), \ldots, l_m(\xi)}\right|.$$

Dans ce qui suit, nous considérerons surtout les r premiers logarithmes de la forme ξ ou du nombre α. Pour ces r premiers logarithmes, on a évidemment

$$\left.\begin{array}{l} l_s(\xi\eta) = l_s(\xi) + l_s(\eta) \\ l_s(\alpha\beta) = l_s(\alpha) + l_s(\beta) \end{array}\right\} \qquad (s = 1, \ldots, r)$$

Nous démontrerons dès lors le

Lemme 9. — Il y a toujours dans le corps k une unité ε qui satisfait à

$$\gamma_1 l_1(\varepsilon) + \ldots + \gamma_r l_r(\varepsilon) \neq 0$$

où $\gamma_1, \gamma_2, \ldots, \gamma_r$ sont des constantes réelles quelconques données qui ne sont pas toutes nulles.

Démonstration. — Soit ω un nombre quelconque du corps qui n'est pas nul; posons pour abréger

$$\mathrm{L}(\omega) = \gamma_1 l_1(\omega) + \ldots + \gamma_r l_r(\omega);$$

déterminons ensuite un système de r grandeurs réelles telles que $\gamma_1\lambda_1 + \ldots + \gamma_r\lambda_r = 1$, et posons

$$\Lambda_1 = e^{\lambda_1 t}, \quad \ldots, \quad \Lambda_{r_1} = e^{\lambda_{r_1} t}, \quad \Lambda_{r_1+1} = e^{\frac{1}{2}\lambda_{r_1+1} t}, \quad \ldots, \quad \Lambda^{\frac{1}{2}\lambda_r t}$$

où t représente un paramètre arbitraire.

Nous distinguerons deux cas suivant que les m corps conjugués $k^{(1)}, \ldots, k^{(m)}$ sont réels ou non. Dans le premier cas, nous attribuerons aux $r = m - 1$ corps $k^{(1)}, \ldots, k^{(r)}$ les grandeurs $\Lambda_1, \ldots, \Lambda_r$ et au dernier corps $k^{(m)}$ la constante

$$\Lambda_m = \frac{|\sqrt{d}|}{\Lambda_1 \ldots \Lambda_{m-1}}.$$

Dans le second cas, nous attribuerons aux corps $k^{(1)}, \ldots, k^{(r)}$ les grandeurs $\Lambda_1, \ldots, \Lambda_r$, et au corps imaginaire $k^{(r+1)}$ nous ferons correspondre

$$\Lambda_{r+1} = \left| \left\{ \frac{\sqrt{d}}{\Lambda_1 \ldots \Lambda_{r_1} \Lambda_{r_1+1}^2 \ldots \Lambda_r^2} \right\}^{\frac{1}{2}} \right|.$$

Enfin, aux $m - r - 1$ corps imaginaires qui restent $k^{(r+2)}, \ldots, k^{(m)}$, nous ferons correspondre les mêmes constantes que celles qui correspondent déjà à leurs conjugués, nous désignerons ces constantes par $\Lambda_{r+2}, \ldots, \Lambda_m$.

Dans les deux cas

$$\Lambda_1 \ldots \Lambda_m = |\sqrt{d}|,$$

et les constantes $\Lambda_1, \ldots, \Lambda_m$ remplissent les conditions imposées aux constantes $\varkappa_1, \varkappa_2, \ldots, \varkappa_m$ du théorème 42.

Il y a donc, suivant ce théorème 42, un nombre α du corps k différent de zéro et tel que

$$(10) \qquad |\alpha^{(1)}| \leqq \Lambda_1, \quad \ldots, \quad |\alpha^{(m)}| \leqq \Lambda_m,$$

et par suite tel que $|n(\alpha)| \leqq |\sqrt{d}|$. Mais comme $|n(\alpha)| \geqq 1$, on a pour toutes les valeurs de $s = 1, 2, \ldots, m$

$$|\alpha^{(s)}| \geqq \frac{1}{|\alpha^{(1)}| \ldots |\alpha^{(s-1)}| |\alpha^{(s+1)}| |\alpha^{(m)}|};$$

si donc nous tenons compte de

$$\left|\frac{1}{\alpha^{(1)}}\right| \geqq \frac{1}{\Lambda_1}, \quad \ldots, \quad \left|\frac{1}{\alpha^{(m)}}\right| \geqq \frac{1}{\Lambda_m}$$

et de

$$\Lambda_1 \ldots \Lambda_m = |\sqrt{d}|$$

il en résulte

$$(11) \qquad |\alpha^{(s)}| \geqq \frac{\Lambda_s}{|\sqrt{d}|}.$$

Désignons la valeur réelle de $\log|\sqrt{d}|$ par δ, (10) et (11) nous donnent

$$\left.\begin{array}{ll} & \lambda_s t \geqq l_s(\alpha) \geqq \lambda_s t - 2\delta \\ \text{ou} & 0 \leqq |l_s(\alpha) - \lambda_s t| \leqq 2\delta \end{array}\right\} \qquad (s = 1, 2, \ldots, r).$$

On voit donc que l'expression

$$\gamma_1\{l_1(\alpha) - \lambda_1 t\} + \ldots + \gamma_r\{l_1(\alpha) - \lambda_r t\} = \mathrm{L}(\alpha) - t$$

est comprise entre deux limites finies δ_1 et $\delta_2 > \delta_1$, qui ne dépendent que de d et des valeurs $\gamma_1, \ldots, \gamma_r$, mais qui ne dépendent pas de la valeur du paramètre t.

Soit une grandeur $\Delta > \delta_2 - \delta_1$ et donnons à t successivement les valeurs $t = 0$, Δ, 2Δ, 3Δ, ..., on obtiendra une suite infinie de nombres α, β, γ, ..., dont les normes prises en valeur absolue sont $\leqq |\sqrt{d}|$ et qui de plus satisfont aux conditions $\mathrm{L}(\alpha) < \mathrm{L}(\beta) < \mathrm{L}(\gamma) < \ldots$.

Comme les nombres rationnels qui en valeur absolue sont $\leqq |\sqrt{d}|$ ne contiennent qu'un nombre fini d'idéaux différents en facteur, la suite illimitée d'idéaux principaux (α), (β), (γ), ... ne peut contenir qu'un nombre limité d'idéaux différents, et par suite on trouvera une infinité de fois dans cette suite deux idéaux égaux. Soit, par exemple $(\alpha) = (\beta)$, alors $\varepsilon = \frac{\beta}{\alpha}$ est une unité, et cette unité, à cause de

$$\mathrm{L}(\varepsilon) = \mathrm{L}(\beta) - \mathrm{L}(\alpha) > 0,$$

remplit les conditions du lemme 9.

§ 20. — Démonstration de l'existence des unités.

Pour démontrer dès lors le théorème 47, nous choisirons dans k une unité η_1 conforme au lemme 9, telle que $l_1(\eta_1) \neq 0$, et ensuite une unité η_2 telle que le déterminant

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2) \\ l_2(\eta_1), & l_2(\eta_2) \end{vmatrix} \neq 0;$$

ensuite une unité η_3 telle que le déterminant

$$\begin{vmatrix} l_1(\eta_1), & l_1(\eta_2), & l_1(\eta_3) \\ l_2(\eta_1), & l_2(\eta_2), & l_2(\eta_3) \\ l_3(\eta_1), & l_3(\eta_2), & l_3(\eta_3) \end{vmatrix} \neq 0;$$

et ainsi de suite, on parvient ainsi finalement au déterminant

$$\begin{vmatrix} l_1(\eta_{1_1}), & \dots, & l_1(\eta_{1_r}) \\ \dots & \dots & \dots \\ l_r(\eta_{1_1}), & \dots, & l_r(\eta_{1_r}) \end{vmatrix} \neq 0.$$

Par suite, si H est une unité quelconque du corps, les r premiers logarithmes peuvent toujours être mis sous la forme

$$\begin{aligned} l_1(\mathrm{H}) &= e_1 l_1(\eta_{1_1}) + \dots + e_r l_1(\eta_{1_r}), \\ &\dots\dots\dots\dots \\ l_r(\mathrm{H}) &= e_1 l_r(\eta_{1_1}) + \dots + e_r l_r(\eta_{1_r}) \end{aligned}$$

où $e_1, \dots, e_r$ sont des grandeurs réelles. Cette représentation montre à son tour que l'on peut écrire

$$\begin{aligned} l_1(\mathrm{H}) &= m_1 l_1(\eta_{1_1}) + \dots + m_r l_1(\eta_{1_r}) + \mathrm{E}_1, \\ &\dots\dots\dots\dots \\ l_r(\mathrm{H}) &= m_1 l_r(\eta_{1_1}) + \dots + m_r l_r(\eta_{1_r}) + \mathrm{E}_r \end{aligned}$$

où $m_1, \dots, m_r$ sont les plus grandes valeurs numériques rationnelles entières contenues dans $e_1, \dots, e_r$. Les nombres $\mathrm{E}_1, \dots, \mathrm{E}_r$ sont à leur tour de la forme

$$\begin{aligned} \mathrm{E}_1 &= \mu_1 l_1(\eta_{1_1}) + \dots + \mu_r l_1(\eta_{1_r}), \\ &\dots\dots\dots\dots \\ \mathrm{E}_r &= \mu_1 l_r(\eta_{1_1}) + \dots + \mu_r l_r(\eta_{1_r}). \end{aligned}$$

Comme ici $\mu_1, \dots, \mu_r$ sont des valeurs réelles $\geqq 0$ et < 1, les valeurs $\mathrm{E}_1, \dots, \mathrm{E}_r$ prises en valeur absolue sont inférieures à une limite $\varkappa$ qui ne dépend pas de H, c'est-à-dire que les r premiers logarithmes de l'unité

$$\overline{\mathrm{H}} = \frac{\mathrm{H}}{\eta_{1_1}^{m_1} \dots \eta_{1_r}^{m_r}}$$

sont tous inférieurs à la limite $\varkappa$. Mais comme

$$l_1(\overline{\mathrm{H}}) + \dots + l_{r+1}(\overline{\mathrm{H}}) = 0,$$

la valeur absolue de $l_{r+1}(\overline{\mathrm{H}})$ est inférieure à $r\varkappa$, et on a les inégalités

$$|\overline{\mathrm{H}}^{(1)}| < e^{\varkappa}, \quad \dots, \quad |\overline{\mathrm{H}}^{(r)}| < e^{\varkappa}, \quad |\overline{\mathrm{H}}^{(r+1)}| < e^{r\varkappa},$$

c'est-à-dire que toutes les valeurs conjuguées de l'unité $\overline{\mathrm{H}}$ sont, en valeur absolue, inférieures à $e^{r\varkappa}$.

D'après le théorème 43, il n'existe qu'un nombre limité de pareilles unités. Désignons-les par $\mathrm{H}_1, \dots, \mathrm{H}_{\mathrm{G}}$; il en résultera $\overline{\mathrm{H}} = \mathrm{H}_{\mathrm{S}}$ ou $\mathrm{H} = \mathrm{H}_{\mathrm{S}} \eta_{1_1}^{m_1} \dots \eta_{1_r}^{m_r}$ où S est l'un des nombres $1, 2, \dots, \mathrm{G}$. Soit H_{Γ} l'une quelconque des unités $\mathrm{H}_1, \dots, \mathrm{H}_{\mathrm{G}}$ et for-

mons les $G+1$ premières puissances de H_T; d'après ce qui vient d'être dit, deux quelconques de ces puissances pourront être mises sous la forme

$$H_S \eta_1^{m'_1} \ldots \eta_r^{m'_r}$$

et

$$H_S \eta_1^{m''_1} \ldots \eta_r^{m''_r}$$

où H_S représente chaque fois la même de ces G unités; leur quotient pourra donc être mis sous la forme $\eta_1^{m_1} \ldots \eta_r^{m_r}$. Nous avons donc démontré qu'à toute unité H^1 correspond un exposant M_T tel que $M_T^{M_T}$ soit un produit de puissance des unités $\eta_1, \ldots, \eta_r$. Soit M le plus petit multiple commun des composants $H_1, \ldots, H_G$, cet exposant G aura la même propriété pour toutes les G unités $H_1, \ldots, H_G$, et il en résultera que les r premiers logarithmes d'une unité quelconque H admettent la représentation

$$(12)\quad \begin{cases} l_1(H) = \dfrac{m_1 l_1(\eta_1) + \ldots + m_r l_1(\eta_r)}{M}, \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ l_r(H) = \dfrac{m_1 l_r(\eta_1) + \ldots + m_r l_r(\eta_r)}{M}, \end{cases}$$

où $m_1, \ldots, m_r$ sont des nombres entiers rationnels.

En appliquant dès lors à ce système illimité de logarithmes de toutes les unités du corps le raisonnement appliqué paragraphe 3 pour le théorème (5) relatif à l'existence de la base du corps, on arrive au résultat suivant. Il y a un système de r unités $\varepsilon_1, \ldots, \varepsilon_r$ telle que les logarithmes d'une unité quelconque H du corps puisse s'exprimer par

$$l_1(H) = a_1 l_1(\varepsilon_1) + \ldots + a_r l_1(\varepsilon_r),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$l_r(H) = a_1 l_r(\varepsilon_1) + \ldots + a_r l_r(\varepsilon_r)$$

où $a_1, \ldots, a_r$ sont des entiers rationnels. Le système d'unités $\varepsilon_1, \ldots, \varepsilon_r$ satisfait aux conditions du théorème 47.

En effet : Soit H une unité quelconque, dont les logarithmes ont la forme précédente. $\rho = \dfrac{H}{\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}}$ est une unité dont les logarithmes sont évidemment tous nuls. Une telle unité ρ est nécessairement une racine de l'unité; car, d'après ce qui a été démontré, $\rho^M = \eta_1^{m_1} \ldots \eta_r^{m_r}$ où $m_1, \ldots, m_r$ sont certains nombres entiers rationnels. En passant aux logarithmes on voit que

$$m_1 l_1(\eta_1) + \ldots + m_r l_1(\eta_r) = 0,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$m_1 l_r(\eta_1) + \ldots + m_r l_r(\eta_r) = 0,$$

c'est-à-dire $m_1 = 0, \ldots, m_r = 0$ et par suite $\rho^M = 1$. L'unité H est donc représentée comme l'exige notre théorème 47.

Il résulte de la façon dont nous avons déterminé $\varepsilon_1, \ldots, \varepsilon_r$ que

$$\begin{vmatrix} l_1(\eta_{11}), & \ldots, & l_1(\eta_{1r}) \\ \cdot & \cdot & \cdot \\ l_r(\eta_{11}), & \ldots, & l_r(\eta_{1r}) \end{vmatrix} = \mathrm{AR},$$

où A est un nombre entier rationnel et où R désigne

$$\mathrm{R} = \begin{vmatrix} l_1(\varepsilon_1), & \ldots, & l_1(\varepsilon_r) \\ \cdot & \cdot & \cdot \\ l_r(\varepsilon_1), & \ldots, & l_r(\varepsilon_r) \end{vmatrix}.$$

Le déterminant $\mathrm{R} \neq 0$, et par suite la représentation de H au moyen des $\varepsilon_1, \ldots, \varepsilon_r$ n'est possible que d'une seule manière.

Le théorème fondamental 47 est donc complètement démontré.

§ 21. — Les unités fondamentales. — Le régulateur du corps. — Un système d'unités indépendantes.

Le système des unités $\varepsilon_1, \ldots, \varepsilon_r$ ayant la propriété dite au théorème 47 est dit un *système d'unités fondamentales* du corps k. Il en résulte facilement que si $\varepsilon_1^*, \ldots, \varepsilon_r^*$ représente un autre système d'unités fondamentales, le déterminant des r systèmes de r logarithmes est égal au signe près à R. Nous écrirons constamment ces unités dans un ordre tel que R soit un nombre positif. Le nombre R est alors parfaitement déterminé dans le corps k et nous le nommerons le *régulateur du corps k*.

Dans le courant de la démonstration précédente nous avons reconnu qu'une unité dont tous les logarithmes sont $= 0$ est une racine de l'unité. Ce fait est contenu dans le théorème suivant, que l'on peut démontrer d'ailleurs d'une façon directe. [Kronecker[6], Minkowski[3].]

Théorème 48. — Toute unité telle que sa valeur absolue égale 1, ainsi que les valeurs de toutes ses conjuguées, est une racine de l'unité.

Tout corps contient les unités $+1$ et -1, le nombre de toutes les racines de l'unité qu'on y rencontre est toujours pair, et il ne peut être > 2 que si tous les m corps conjugués sont imaginaires.

On dit qu'un système de t unités $\eta_{11}, \ldots, \eta_{1t}$ forme *un système de t unités indépendantes* s'il n'existe entre ces unités aucune relation de la forme $\eta_{11}^{m_1} \ldots \eta_{1t}^{m_t} = 1$ où $m_1, \ldots, m_t$ sont des nombres entiers rationnels qui ne sont pas tous nuls; t est toujours [illegible] r. En particulier les unités fondamentales $\varepsilon_1, \ldots, \varepsilon_r$ forment un système de r unités indépendantes. Si l'on a, d'autre part, un système quelconque de r unités indépendantes $\eta_{11}, \ldots, \eta_{1r}$, il existe toujours un entier rationnel M tel que

$$\varepsilon^{\mathrm{M}} = \eta_{11}^{m_1} \ldots \eta_{1r}^{m_r}$$

où les exposants $m_1, \dots, m_r$ sont des entiers rationnels ; car si $\eta_s = \rho_s \varepsilon_1^{a_{s1}} \dots \varepsilon_r^{a_{sr}}$ pour $s = 1, 2, \dots, r$ où les ρ_s désignent des racines de l'unité et où $a_{11}, \dots, a_{rr}$ sont des exposants entiers et rationnels, le déterminant A formé par ces exposants entiers $a_{11}, \dots, a_{rr}$ est nécessairement $\neq 0$, et cela en vertu de l'hypothèse sur l'indépendance des unités $\eta_1, \dots, \eta_r$. La $A^{\text{ième}}$ puissance de toute unité ε du corps est égale à un produit de puissance des $\eta_1, \dots, \eta_r$ multiplié par une racine de l'unité ρ. Soit $\rho^E = 1$ pour toutes les racines de l'unité dans k le nombre $M = AE$ aura la propriété demandée.

La démonstration de notre théorème fondamental 47 nous a montré la possibilité d'obtenir les unités fondamentales $\varepsilon_1, \dots, \varepsilon_r$ par un nombre limité d'opérations rationnelles. Lorsqu'on cherche à calculer ces unités de la façon la plus simple on est conduit à un algorithme semblable aux fractions continues, et ce qui forme alors le principal intérêt de la question c'est la périodicité des développements obtenus. [Minkowski[3,4].]

CHAPITRE VII.

Les classes d'idéaux des corps.

§ 22. — LA CLASSE DES IDÉAUX. — LE NOMBRE DES CLASSES D'IDÉAUX EST LIMITÉ.

Tout nombre entier du corps k détermine un idéal principal. Tout nombre fractionnaire $\varkappa$ de k peut être représenté par le quotient de deux nombres entiers α et β et par suite par le quotient de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$ $\varkappa = \frac{\alpha}{\beta} = \frac{\mathfrak{a}}{\mathfrak{b}}$.

Si nous supposons $\mathfrak{a}$ et $\mathfrak{b}$ débarrassés de tous leurs facteurs idéaux communs, la représentation du nombre $\varkappa$ par un quotient de deux idéaux est unique. Réciproquement, si le quotient $\frac{\mathfrak{a}}{\mathfrak{b}}$ de deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, que ceux-ci aient un facteur commun ou non, est égal au nombre entier ou à un nombre fractionnaire $\varkappa = \frac{\alpha}{\beta}$ du corps, on dit que les deux idéaux $\mathfrak{a}$ *et* $\mathfrak{b}$ *sont équivalents*, ce qu'on écrit $\mathfrak{a} \sim \mathfrak{b}$. De $\frac{\alpha}{\beta} = \frac{\mathfrak{a}}{\mathfrak{b}}$ il résulte $(\beta)\mathfrak{a} = (\alpha)\mathfrak{b}$.

Nous reconnaîtrons donc que deux idéaux sont équivalents si en multipliant l'un et l'autre par certains idéaux principaux on obtient un même idéal. L'ensemble des idéaux équivalents à un même idéal forme une *classe d'idéaux*.

Tous les idéaux principaux sont équivalents à l'idéal (1). La classe obtenue ainsi s'appelle la *classe principale* et on la désigne par 1. Si $\mathfrak{a} \sim \mathfrak{a}'$ et $\mathfrak{b} \sim \mathfrak{b}'$, on a $\mathfrak{a}\mathfrak{a}' \sim \mathfrak{b}\mathfrak{b}'$.

Soit A une classe qui contient $\mathfrak{a}$, et B une classe qui contient $\mathfrak{b}$. La classe qui contient $\mathfrak{ab}$ est dite le *produit des classes* A et B, et on les désigne par AB.

On a évidemment $1 . B = B$, et réciproquement.

Si $A . B = B$, on a nécessairement $A = 1$.

Il est parfois avantageux d'employer la notation de quotients d'idéaux. Nous conviendrons que

$$\frac{\mathfrak{a}}{\mathfrak{a}'} = \frac{\mathfrak{b}}{\mathfrak{b}'} \quad \text{ou} \quad \frac{\mathfrak{a}}{\mathfrak{a}'} \sim \frac{\mathfrak{b}}{\mathfrak{b}'}$$

équivaut à $\mathfrak{ab}' = \mathfrak{a}'\mathfrak{b}$ ou $\mathfrak{ab}' \sim \mathfrak{a}'\mathfrak{b}$.

Théorème 49. — Il y a toujours une classe B et une seule dont le produit par une classe A donnée est la classe principale.

Démonstration. — Soit $\mathfrak{a}$ un idéal de la classe A et α un nombre divisible par $\mathfrak{a}$, de façon que $\alpha = \mathfrak{ab}$; soit alors B la classe de l'idéal $\mathfrak{b}$, on a $AB = 1$. S'il existait une autre classe B' telle que $AB' = 1$, on aurait $ABB' = B' = B$.

La classe B est dite la *classe réciproque* de A; on la désigne par A^{-1}.

On a de plus le fait fondamental suivant :

Théorème 50. — Il y a dans toute classe d'idéaux un idéal dont la norme est inférieure à la valeur absolue de la racine carrée du discriminant du corps. [Minkowski [1,3].] Le nombre des classes d'idéaux du corps de nombres est fini. [Dedekind [1], Kronecker [10].]

Démonstration. — Soit A une classe quelconque et soit $\mathfrak{j}$ un idéal de la classe réciproque A^{-1}; on sait d'après le théorème 46 qu'il existe un nombre entier ι divisible par $\mathfrak{j}$ dont la norme $|n(\iota)| \leqq n(\mathfrak{j}) \left|\sqrt{d}\right|$. Soit $\iota = \mathfrak{ja}$, $\mathfrak{a}$ appartient à la classe A, et comme $|n(\iota)| = (\mathfrak{j}) n(\mathfrak{a})$, on a $n(\mathfrak{a}) \leqq \left|\sqrt{d}\right|$. Mais comme les nombres entiers rationnels $\leqq \left|\sqrt{d}\right|$ ne contiennent qu'un nombre fini d'idéaux en facteurs, la deuxième partie du théorème 50 est démontrée.

§ 23. — Une application du théorème sur le nombre fini des classes.

Le théorème 50 que nous venons de démontrer permet bien des déductions, dont nous signalerons les suivantes :

Théorème 51. — Si h est le nombre des classes d'idéaux, la $h^{\text{ième}}$ puissance de toute classe donne la classe principale.

Démonstration. — Considérons la suite $A, A^2, \ldots, A^{h+1}$; deux classes de cette suite coïncident nécessairement, soient A^r et A^{r+e}, comme $A^r A^e = A^r$, $A^e = 1$; il en résulte

que $A^e = 1$, A, ..., A^{e-1} sont toutes différentes entre elles. Soit B une classe différente des e précédentes; B, AB, ..., $A^{e-1}B$ nous donnent e classes nouvelles différentes entre elles et différentes des précédentes; en continuant on voit que h est un multiple de e, ce qui démontre le théorème 51.

La $h^{\text{ième}}$ puissance d'un idéal $\mathfrak{a}$ est donc toujours un idéal principal.

Théorème 52. — Soient α et β deux entiers quelconques, il y a toujours un nombre entier γ différent de 0 qui divise α et β et susceptible d'être mis sous la forme $\gamma = \xi\alpha + \eta\beta$ où ξ et η sont des nombres convenablement choisis. Les nombres γ, ξ, η n'appartiennent pas en général au corps déterminé par α et β. [Dedekind[1].]

Théorème 53. — Pour que $\varkappa$ et ρ, $\varkappa^*$ et ρ^* soient deux couples de nombres du corps k tels que $\mathfrak{j} = (\varkappa, \rho) = (\varkappa^*, \rho^*)$, il est nécessaire et suffisant que l'on puisse trouver dans le corps k quatre nombres entiers α, β, γ, δ dont le déterminant $\alpha\delta - \beta\gamma = 1$ et tels que

$$\varkappa^* = \alpha\varkappa + \beta\rho,$$
$$\rho^* = \gamma\varkappa + \delta\rho.$$

[Hurwitz[4].]

Démonstration. — La condition est suffisante, car les équations précédentes permettent d'écrire

$$\varkappa = \alpha^*\varkappa^* + \beta^*\rho^*,$$
$$\rho = \gamma^*\varkappa^* + \delta^*\rho^*$$

où α^*, β^*, γ^*, δ sont entiers. De plus, la condition est nécessaire, car si l'on désigne par h le nombre des classes d'idéaux on a $\mathfrak{j}^h = (\varkappa^h, \rho^h) = (\varkappa^{*h}, \rho^{*h}) = (\tau)$ où τ est un entier du corps. Soit

$$\tau = \mu\varkappa^h + \nu\rho^h = \mu^*\varkappa^{*h} + \nu^*\rho^{*h}$$

où μ, ν, μ^*, ν^* sont des entiers de k; alors il est évident que les quatre entiers

$$\alpha = \frac{\mu\varkappa^*\varkappa^{h-1} + \nu^*\rho\rho^{*h-1}}{\tau}, \qquad \beta = \frac{\nu\varkappa^*\rho^{h-1} - \nu^*\varkappa\rho^{*h-1}}{\tau},$$

$$\gamma = \frac{\mu\rho^*\varkappa^{h-1} - \mu^*\rho\varkappa^{*h-1}}{\tau}, \qquad \delta = \frac{\nu\rho^*\rho^{h-1} + \mu^*\varkappa\varkappa^{*h-1}}{\tau}$$

satisfont aux conditions du théorème 53. On voit que $\alpha\delta - \beta\gamma = 1$ en faisant le produit des déterminantes

$$-\tau = \begin{vmatrix} \mu\varkappa^{h-1}, & \rho \\ \nu\rho^{h-1}, & -\varkappa \end{vmatrix} \quad \text{et} \quad -\tau = \begin{vmatrix} \varkappa^*, & \nu^*\rho^{*h-1} \\ \rho^*, & -\mu^*\varkappa^{*h-1} \end{vmatrix}$$

D'après le théorème 12, tout idéal peut être mis sous la forme $\mathfrak{j} = (\varkappa, \rho)$. Posons $\theta = \frac{\varkappa}{\rho}$: le nombre entier ou fractionnaire θ détermine complètement la classe d'idéaux

à laquelle appartient $\mathfrak{j}$. Nous dirons que θ est le *nombre fractionnaire* attribué à la classe d'idéaux. Le théorème 53 nous montre que si $\theta^* = \frac{\alpha^*}{\rho^*}$ est une autre fraction attribuée à cette classe d'idéaux, il existe dans le corps k nécessairement quatre nombres $\alpha, \beta, \gamma, \delta$ de déterminants 1 tels que $\theta^* = \frac{\alpha\theta + \beta}{\gamma\theta + \delta}$.

§ 24. — Comment on établit le système des classes d'idéaux. — Sens plus restreint de la notion de classe.

La démonstration du théorème 50 nous donne un moyen simple de trouver par un nombre fini d'opérations rationnelles un système complet d'idéaux qui ne soient pas équivalents. Il suffit de considérer tous les idéaux dont la norme $\leqslant |\sqrt{d}|$. Pour voir s'il y a parmi ces idéaux des idéaux équivalents il suffit de former tous les produits deux à deux; soit $\mathfrak{j}$ un de ces produits, cherchons dans $\mathfrak{j}$ un nombre $\iota \neq 0$ et de norme minima en valeur absolue, il suffira de voir si $\mathfrak{j} = (\iota)$ et de reconnaître ainsi si les deux facteurs appartiennent à des classes réciproques. Le théorème 46 nous montre que ceci pourra s'effectuer par un nombre limité d'opérations. Soit $\iota_1, \ldots, \iota_m$ la base de l'idéal $\mathfrak{j}$, il suffit de déterminer pour $u_1, \ldots, u_m$ des valeurs entières rationnelles $\neq 0$ telles que les valeurs absolues des parties réelles et des parties imaginaires de $u_1\iota_1^{(s)} + \ldots + u_m\iota_m^{(s)}$ pour $s = 1, \ldots, m$ soient toutes inférieures à des limites déterminées. Il suffit pour cela d'un nombre limité d'opérations. Nous verrons de même qu'étant donné un idéal un nombre limité d'opérations rationnelles permet de déterminer la classe auquel il appartient.

Nous remarquerons que dans certaines circonstances il pourra être utile de considérer *un sens restreint de la notion d'équivalence ou de classes*, et on dira alors que deux idéaux ne sont équivalents que si leur quotient est un nombre entier ou fractionnaire de norme positive. [Dedekind [1].]

§ 25. — Un théorème auxiliaire relatif à la valeur asymptotique du nombre de tous les idéaux principaux qui sont divisibles par un idéal donné.

Dirichlet a exprimé le nombre des classes des formes binaires de déterminant donné par une voie transcendante. [Dirichlet [7, 8].] Dedekind, suivant son exemple et en se basant sur les résultats du chapitre VI concernant les unités d'un corps, parvint à établir une formule fondamentale à l'aide de laquelle le nombre h des classes d'idéaux d'un corps quelconque se présente comme la limite d'une certaine série infinie. [Dedekind [1].] Pour atteindre cette formule nous démontrerons tout d'abord le théorème suivant :

Lemme 10. — Si t est une certaine variable positive et T le nombre de tous les idéaux principaux divisibles par $\mathfrak{a}$ dont la norme $\leqslant t$, on a

$$\underset{t=\infty}{\mathrm{L}} \frac{\mathrm{T}}{t} = \frac{2^{r_1+r_2}\pi^{r_2}}{w} \cdot \frac{1}{n(\mathfrak{a})} \frac{\mathrm{R}}{|\sqrt{d}|}$$

où w est le nombre des racines de l'unité que l'on rencontre dans k et où R désigne le régulateur du corps. r_1, r_2 ont le sens indiqué au théorème 47. L signifie limite.

Démonstration. — Soit $\alpha_1, \ldots, \alpha_m$ une base de l'idéal $\mathfrak{a}$; tout nombre entier divisible par $\mathfrak{a}$ est de la forme

$$\eta = \eta(v) = v_1\alpha_1 + \ldots + v_m\alpha_m = f_1(v)\omega_1 + \ldots + f_m(v)\omega_m$$

où $v_1, \ldots, v_m$ sont des entiers rationnels et $f_1(v), \ldots, f_m(v)$ sont des formes linéaires à coefficients entiers rationnels des $v_1, \ldots, v_m$.

Considérons les $v_1, \ldots, v_m$ comme des variables réelles et posons

$$u_1 = \frac{f_1(v)}{|\sqrt[m]{n(\eta)}|}, \quad \ldots, \quad u_m = \frac{f_m(v)}{|\sqrt[m]{n(\eta)}|},$$

$$\xi = \xi(v) = u_1\omega_1 + \ldots + u_m\omega_m = \frac{\eta(v)}{|\sqrt[m]{n(\eta)}|},$$

$u_1, \ldots, u_m$ seront des fonctions bien déterminées de $v_1, \ldots, v_m$ et ξ est une forme pour laquelle $n(\xi) = \pm 1$. Nous calculerons les r premiers logarithmes de la forme ξ et de là nous tirerons r grandeurs réelles $e_1(\xi), \ldots, e_r(\xi)$ telles qu'en désignant par $\varepsilon_1, \ldots, \varepsilon_r$ un système d'unités fondamentales on ait

$$l_1(\xi) = e_1(\xi)l_1(\varepsilon_1) + \ldots + e_r(\xi)l_1(\varepsilon_r),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$l_r(\xi) = e_1(\xi)l_r(\varepsilon_1) + \ldots + e_r(\xi)l_r(\varepsilon_r);$$

nous dirons dans le courant de ce § 25 que ces grandeurs $e_1, \ldots, e_r$ sont les exposants de η.

Si l'on prend pour les $v_1, \ldots, v_m$ des valeurs entières rationnelles qui ne sont pas toutes nulles, il est évident que le nombre η ainsi obtenu peut être transformé en le multipliant par des puissances des unités $\varepsilon_1, \ldots, \varepsilon_r$ en un nombre dont les exposants $e_1, \ldots, e_r$ satisfont à

(13) $$0 \leqslant e_1 < 1, \quad \ldots, \quad 0 \leqslant e_r < 1.$$

Réciproquement, on voit que deux nombres η, η^* dont les exposants sont égaux ne peuvent différer que par un facteur qui est une racine de l'unité. Si donc le nombre des racines de l'unité situées dans k est w, wT où T est le nombre des idéaux principaux divisibles par $\mathfrak{a}$ et de norme $\leqslant t$ est égal au nombre des systèmes de

valeurs numériques entières différentes des $v_1, \ldots, v_m$ tels que $n(\eta) \leqq t$ et telles que les exposants $e_1, \ldots, e_r$ satisfassent à (13).

Posons

$$\tau = t^{-\frac{1}{m}}, \quad v_1 = \frac{\varphi_1}{\tau}, \quad \ldots, \quad v_m = \frac{\varphi_m}{\tau};$$

la forme ξ et par suite les grandeurs $l_1(\xi), \ldots, l_r(\xi), e_1, \ldots, e_r$ resteront indépendantes de τ et contiendront seulement les m nouvelles variables $\varphi_1, \ldots, \varphi_m$. L'inégalité $|n(\eta)| \leqq t$ devient $\left|n\big(\eta(\varphi)\big)\right| \leqq 1$; de plus, en vertu de (13), les r logarithmes $l_1(\xi), \ldots, l_r(\xi)$ et à cause de $l_1(\xi) + \ldots + l_{r+1}(\xi) = ln(\xi) = 0$; aussi $l_{r+1}(\xi)$ sont tous en valeur absolue inférieurs à certaines limites finies déterminées par les $\varepsilon_1, \ldots, \varepsilon_r$; il en résulte qu'il en est de même pour toutes les grandeurs $|\xi^{(1)}(\xi)|, \ldots, |\xi^{(m)}(\varphi)|$ et par suite à cause de $\left|n\big(\eta(\varphi)\big)\right| < 1$ les m grandeurs $|\eta^{(1)}(\varphi)|, \ldots, |\eta^{(m)}(\varphi)|$ sont inférieures à des limites finies. Il en résulte que les conditions (13), en y adjoignant l'inégalité $\left|n\big(\eta(\varphi)\big)\right| \leqq 1$, définissent un espace limité dans l'espace à m dimensions déterminé par les m coordonnées $\varphi_1, \ldots, \varphi_m$.

Rappelons que nous avons vu au § 19 que les valeurs fonctionnelles $l_1(\eta), \ldots, l_r(\eta)$ nous donnent 2^{r_1} déterminations des variables $\varphi_1, \ldots, \varphi_m$; d'après la définition de l'intégrale multiple on a

$$\underset{\tau=0}{\mathrm{L}} \left\{ w\mathrm{T}\tau^m \right\} = 2^{r_1} \int \int \ldots \int d\varphi_1 d\varphi_2 \ldots d\varphi_m,$$

où il faut étendre l'intégration à tout le volume déterminé par

$$0 \leqq e_1 \leqq 1, \quad \ldots, \quad 0 \leqq e_r \leqq 1, \quad \left|n\big(\eta(\varphi)\big)\right| \leqq 1$$

dans l'espace à m dimensions.

Pour déterminer la valeur de cette intégrale qui est finie, nous ferons le changement de variables suivant : nous prendrons pour nouvelles variables

$$\psi_1 = e_1(\xi), \quad \ldots, \quad \psi_r = e_r(\xi),$$
$$\psi_{r+1} = |n(\eta)|, \quad \psi_{r+2} = l_{r+2}(\xi), \quad \ldots, \quad \psi_m = l_m(\xi)$$

où ξ et η dépendent de $\varphi_1, \ldots, \varphi_m$.

Ces m grandeurs sont toutes des fonctions analytiques, uniformes et régulières de $\varphi_1, \ldots, \varphi_m$ à l'intérieur du domaine d'intégration

$$0 \leqq \psi_1 \leqq 1, \quad \ldots, \quad 0 \leqq \psi_r \leqq 1, \quad 0 \leqq \psi_{r+1} \leqq 1,$$
$$0 \leqq \psi_{r+2} \leqq 2\pi, \quad \ldots, \quad 0 \leqq \psi_m \leqq 2\pi.$$

On a donc

$$\int \ldots \int d\varphi_1 \ldots d\varphi_m = \int \ldots \int \left| \frac{\varphi_1, \ldots, \varphi_m}{\psi_1, \ldots, \psi_m} \right| d\psi_1 \ldots d\psi_m.$$

D'après les calculs du § 19,

$$\left|\frac{f_1,\ \ldots,\ f_m}{l_1(\eta),\ \ldots,\ l_m(\eta)}\right| = \left|\frac{n(\eta)}{\sqrt{d}}\right|;$$

de plus, comme

$$ln(\eta) = l_1(\eta) + \ldots + l_{r+1}(\eta), \qquad \underset{(s=1,2,\ldots,r)}{l_s(\xi) = l_s(\eta) - \frac{1}{m}\, ln(\eta)},$$

on a

$$\left|\frac{l_1(\eta),\ \ldots,\ l_r(\eta)\, l_{r+1}(\eta)}{l_1(\eta),\ \ldots,\ l_r(\eta),\ ln(\eta)}\right| = 1, \qquad \left|\frac{l_1(\eta),\ \ldots,\ l_r(\eta),\ ln(\eta)}{l_1(\xi),\ \ldots,\ l_r(\xi),\ ln(\eta)}\right| = 1;$$

et comme enfin

$$l_{r+1}(\eta) = l_{r+1}(\xi), \qquad \ldots, \qquad l_m(\eta) = l_m(\xi),$$

$$\left|\frac{ln(\eta)}{n(\eta)}\right| = \frac{1}{|n(\eta)|}, \qquad \left|\frac{\varphi_1,\ \ldots,\ \varphi_m}{f_1(\varphi),\ \ldots,\ f_m(\varphi)}\right| = \frac{1}{n(\mathfrak{a})}, \qquad \left|\frac{l_1(\xi),\ \ldots,\ l_r(\xi)}{\psi_1,\ \ldots,\ \psi_r}\right| = \mathrm{R},$$

on voit que

$$\left|\frac{\varphi_1,\ \ldots,\ \varphi_m}{\psi_1,\ \ldots,\ \psi_m}\right| = \frac{\mathrm{R}}{n(\mathfrak{a})\left|\sqrt{d}\right|}.$$

L'intégrale précédente a donc la valeur $\dfrac{(2\pi)^{r_2}\mathrm{R}}{n(\mathfrak{a})\left|\sqrt{d}\right|}$, ce qui démontre le théorème auxiliaire.

Dans ce qui suit nous poserons

$$\varkappa = \frac{2^{r_1-r_2}\pi^{r_2}}{w} \cdot \frac{\mathrm{R}}{\left|\sqrt{d}\right|},$$

de sorte que $\varkappa$ est une grandeur déterminée par le corps k seul; et cette grandeur $\varkappa$ caractérise le corps k.

§ 26. — La détermination du nombre des classes par le résidu de $\zeta(s)$ pour $s = 1$.

Théorème 54. — Si l'on désigne par T le nombre de tous les idéaux d'une classe A dont les normes sont $\leqslant t$, on a

$$\underset{t=\infty}{\mathrm{L}} \frac{\mathrm{T}}{t} = \varkappa.$$

Démonstration. — Soit $\mathfrak{a}$ un idéal de la classe A^{-1} réciproque de A, et supposons que $\mathfrak{r}$ représente successivement tous les idéaux de la classe A, le produit $\mathfrak{ra}$ représentera tous les idéaux principaux divisibles par $\mathfrak{a}$, et ne représentera qu'une fois chacun d'eux. Si donc dans la formule du lemme 10 nous remplaçons τ par $t = n(\mathfrak{a})t'$,

T représentera aussi le nombre des idéaux $\mathfrak{r}$ de A pour lesquels $n(\mathfrak{r}) < t'$. En divisant par $n(\mathfrak{a})$ nous aurons la formule que nous voulons démontrer pour $t = t'$.

Comme le nombre $\varkappa$ est indépendant du choix de la classe A, le théorème 54 nous amène immédiatement au

Théorème 55. — Si l'on désigne par T le nombre de tous les idéaux du corps k dont les normes sont $\leqslant t$, et si l'on désigne par h le nombre des classes d'idéaux, on a

$$\mathop{\mathrm{L}}_{t=\infty} \frac{\mathrm{T}}{t} = h\varkappa.$$

On peut, par des méthodes analytiques, déduire de cette formule une expression fondamentale pour h.

Théorème 56. — La série illimitée

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s},$$

où $\mathfrak{j}$ parcourt tous les idéaux du corps, converge pour les valeurs réelles de $s > 1$, et on a

$$\mathop{\mathrm{L}}_{s=1} \{(s-1)\zeta(s)\} = h\varkappa.$$

[Dedekind[1].]

Démonstration. — Désignons par $\mathrm{F}(n)$ le nombre des idéaux différents de norme on a évidemment, si T a la même signification qu'au théorème 55,

$$\mathop{\mathrm{L}}_{t=\infty} \frac{\mathrm{T}}{t} = \mathop{\mathrm{L}}_{n=\infty} \frac{\mathrm{F}(1) + \mathrm{F}(2) + \ldots + \mathrm{F}(n)}{n}.$$

La limite du second membre peut être considérée, comme nous allons le voir, comme la valeur limite d'une série illimitée. [Dirichlet[15].] Nous ordonnerons tous les idéaux $\mathfrak{j}$ du corps d'après la grandeur de leurs normes, nous écrirons la suite $\mathfrak{j}_1, \mathfrak{j}_2, \ldots, \mathfrak{j}_t, \ldots$ et nous désignerons la norme de $\mathfrak{j}_t$ par n_t; alors

$$\mathrm{F}(1) + \ldots + \mathrm{F}(n_t - 1) < t \leqslant \mathrm{F}(1) + \ldots + \mathrm{F}(n_t)$$

ou

$$\frac{\mathrm{F}(1) + \ldots + \mathrm{F}(n_t - 1)}{n_t - 1}\left(1 - \frac{1}{n_t}\right) < \frac{t}{n_t} \leqslant \frac{\mathrm{F}(1) + \ldots + \mathrm{F}(n_t)}{n_t};$$

il en résulte, d'après le théorème 55,

$$\mathop{\mathrm{L}}_{t=\infty} \frac{t}{n_t} = h\varkappa,$$

c'est-à-dire qu'étant donné la grandeur positive δ aussi petite que l'on veut il est toujours possible de choisir un nombre entier t assez grand pour que

$$(14) \qquad \frac{h\varkappa - \delta}{t'} < \frac{1}{n_{t'}} < \frac{h\varkappa + \delta}{t'}$$

pour tous les nombres $t' \geqq t$.

D'autre part, on sait que si s désigne un nombre réel > 1, la suite

$$\sum_{(t)} \frac{1}{t^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots$$

est convergente et que

$$\mathrm{L}_{s=1} \left\{ (s-1) \sum_{(t)} \frac{1}{t^s} \right\} = 1.$$

La dernière égalité nous montre que

$$\mathrm{L}_{s=1} \left\{ (s-1) \sum_{t'} \frac{1}{t'^s} \right\} = 1,$$

lorsque t' parcourt toutes les valeurs supérieures à un nombre donné. De plus, l'inégalité $\frac{1}{n_{t'}} < \frac{h\varkappa + \delta}{t'}$ nous permet de conclure la convergence de la série

$$\sum_{(t)} \frac{1}{n_t^s} = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s}$$

pour $s > 1$, t prenant toutes les valeurs entières positives et $\mathfrak{j}$ représentant successivement tous les idéaux du corps k.

De plus, les inégalités (14) nous donnent la formule

$$(h\varkappa - \delta)^s (s-1) \sum_{(t')} \frac{1}{t'^s} < (s-1) \sum_{(t')} \frac{1}{n_{t'}^s} < (h\varkappa + \delta)^s (s-1) \sum_{(t')} \frac{1}{t'^s}$$

où les sommations s'étendent à toutes les valeurs entières t' qui sont $\geqq t$. Passant à la limite pour $s = 1$, on voit que

$$h\varkappa - \delta \leqq \mathrm{L}_{s=1} \left\{ (s-1) \sum_{(t')} \frac{1}{n_{t'}^s} \right\} \leqq h\varkappa + \delta.$$

Mais on a

$$\mathrm{L}_{s=1} \left\{ (s-1) \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} \right\} = \mathrm{L}_{s=1} \left\{ (s-1) \sum_{(t)} \frac{1}{n_t^s} \right\} = \mathrm{L}_{s=1} \left\{ (s-1) \sum_{(t')} \frac{1}{n_{t'}^s} \right\},$$

et cette limite est à la fois $\geqq h\varkappa - \delta$ et $\leqq h\varkappa + \delta$, et comme δ est un nombre aussi petit que l'on veut, cette limite $= h\varkappa$.

Le théorème 56 est démontré.

§ 27. — On a d'autres développements de $\zeta(s)$.

$\zeta(s)$ peut encore être représentée de trois autres façons différentes :

$$\zeta(s) = \sum_{(n)} \frac{F(n)}{n^s};$$

$$= \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}};$$

$$= \prod_{(p)} \left(\frac{1}{1 - p^{-f_1 s}} \cdot \frac{1}{1 - p^{-f_2 s}} \cdots \frac{1}{1 - p^{-f_e s}} \right).$$

Dans la première expression la sommation s'étend à tous les nombres entiers rationnels pris pour n; dans la deuxième expression le produit s'étend à tous les idéaux premiers du corps; dans la troisième il s'étend à tous les nombres premiers du corps, $f_1, f_2, \ldots, f_e$ désignant les degrés des idéaux premiers contenus dans p. Toutes ces sommes et ces produits infinis convergent pour $s > 1$, et comme les termes sont tous positifs, la convergence ne dépend pas de l'ordre des termes.

§ 28. — La composition des classes d'idéaux d'un corps.

Nous établirons le théorème suivant qui concerne la représentation des classes d'idéaux par des produits. [Schering[1], Kronecker[11].]

Théorème 57. — Il y a toujours q classes $A_1, \ldots, A_q$ telles que toute autre classe A puisse être mise sous la forme $A = A_1^{x_1}, \ldots, A_q^{x_q}$ et cela d'une seule manière; $x_1 \ldots, x_q$ prennent les valeurs entières $0, 1, 2, \ldots$ jusqu'à $h_1 - 1, \ldots, h_{q-1}$, et on a $A_q^{h_q} = 1, \ldots, A_q^{h_q} = 1$ et $h = h_1 \ldots h_q$.

Démonstration. — Cherchons pour chaque classe le plus petit exposant e_1 tel que $A^{e_1} = 1$. Soit h_1 le plus grand de ces exposants e_1 et soit H_1 une classe donnant l'exposant h_1. Cherchons maintenant pour chaque classe le plus petit exposant e_2 tel que A^{e_2} soit une puissance de H_2. Soit h_2 le plus grand de ces e_2 et soit H_2 une classe donnant l'exposant h_2. Cherchons maintenant pour chaque classe A le plus petit exposant $e_3 > 0$ tel que A^{e_3} soit un produit de puissance des classes H_1, H_2; soit h_3 le plus grand de ces e_3 et H_3 une classe donnant h_3. Si l'on continue ainsi on voit que l'on obtient une suite de classes $H_1, H_2, \ldots, H_q$ qui ont la propriété suivante :

Toute classe A peut être mise d'une façon et d'une seule sous la forme

$$A = H_1^{x_1} \ldots H_q^{x_q}$$

$x_1, \ldots, x_q$ ayant les valeurs indiquées au théorème 57.

Soit

$$H_s^{h_s} = H_t^{a_t} H_{t-1}^{a_{t-1}} \dots H_1^{a_1} \tag{15}$$

où $t < s$ et où $a_t, a_{t-1}, \dots, a_1$ sont certains exposants entiers.

D'après nos conventions

$$H_t^{h_t} = H_{t-1}^{b_{t-1}} \dots H_1^{b_1}$$

où $b_{t-1}, \dots, b_1$ sont certains nombres entiers, il faut donc que h_t soit divisible par h_s sans quoi il y aurait une puissance moindre que la $h_s^{\text{ième}}$ de H_s qui pourrait être représentée par un produit des classes $H_t, H_{t-1}, \dots, H_1$.

Soit $h_t = h_s l_s$; il en résulte que $H_t^{a_t l_t}$ est représentable par un produit des classes $H_{t-1}, \dots, H_1$, c'est-à-dire que $a_t l_t$ est divisible par h_t ou que a_t est divisible par h_s. Posons $a_t = h_s c_s$, et, au lieu de choisir H_s, choisissons la classe $H'_s = H_s H_t^{-c_s}$: l'égalité (15) devient

$$H_s'^{h_s} = H_{t-1}^{a_{t-1}} \dots H_1^{a_1}$$

En continuant nous arriverons à remplacer H_s par une classe A_s telle que $A_s^{h_s} = 1$.

On peut, de plus, faire en sorte que dans ce mode de représentation les nombres $h_1, \dots, h_q$ soient des nombres premiers ou des puissances de nombres premiers. Soit $g = p'p'' \dots$ où $p'p''$ sont des puissances de nombres premiers différents; on posera, si B est la classe appartenant à g,

$$B' = B^{\frac{g}{p'}}, \quad B'' = B^{\frac{g}{p''}}, \quad \dots,$$

nous aurons alors $B'^{p'} = 1$, $B'^{p''} = 1$, ..., et si l'on écrit

$$\frac{1}{g} = \frac{a'}{p'} + \frac{a''}{p''} + \dots,$$

on aura $B = B'^{a'} B''^{a''} \dots$. On pourra introduire $B', B'', \dots$ au lieu de B.

Lorsque les classes A sont choisies de la manière qui vient d'être indiquée, on dit qu'elles forment un *système de classes fondamentales.*

§ 29. — Les caractères d'une classe d'idéaux. — Une généralisation de la fonction $\zeta(s)$.

Supposons que l'on ait choisi un système de classes fondamentales, toute classe se trouvera bien déterminée par les exposants $x_1, \dots, x_q$ et par suite par les q racines de l'unité

$$\chi_1(A) = e^{\frac{2i\pi x_1}{h_1}}, \quad \dots, \quad \chi_r(A) = e^{\frac{2i\pi x_r}{h_r}}.$$

Ces q racines de l'unité $\chi(A)$ sont dites *les caractères de la classe* A. Si $\chi(A)$ et $\chi(B)$ sont des caractères de A et de B, $\chi(AB)=\chi(A)\chi(B)$. Le caractère $\chi(A)$ d'une classe est aussi considéré comme le caractère $\chi(\mathfrak{a})$ de tout idéal $\mathfrak{a}$ contenu dans A.

A l'aide des caractères on peut former une fonction qui est une généralisation de la fonction $\zeta(s)$ que l'on vient de considérer et qui admet un semblable développement en produit infini. [Dedekind[1].] Cette fonction est

$$\sum_{(\mathfrak{j})} \frac{\chi(\mathfrak{j})}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1-\chi(\mathfrak{p})\, n(\mathfrak{p})^{-s}}$$

où la somme s'étend à tous les idéaux $\mathfrak{j}$ du corps k et le produit à tous ses idéaux premiers $\mathfrak{p}$.

CHAPITRE VIII.

Les formes décomposables du corps.

§ 30. — Les formes décomposables du corps. — Les classes de formes et leur composition.

Soient $\xi^{(1)}, \ldots, \xi^{(m)}$ m formes linéaires des m variables $u_1, \ldots, u_m$ avec des coefficients quelconques réels ou imaginaires, le produit

$$U(u_1, \ldots, u_m) = \xi^{(1)} \ldots \xi^{(m)}$$

est dit une *forme décomposable* de degré m des m variables $u_1, \ldots, u_m$. Les coefficients des produits de $u_1, \ldots, u_m$ sont dits les *coefficients de la forme*. Si l'on tient compte des formules

$$-\frac{\partial^2 \log U}{\partial u_r \partial u_s} = \frac{\partial \log \xi^{(1)}}{\partial u_r}\frac{\partial \log \xi^{(1)}}{\partial u_s} + \ldots + \frac{\partial \log \xi^{(m)}}{\partial u_r}\frac{\partial \log \xi^{(m)}}{\partial u_s}, \quad (r, s = 1, \ldots, m)$$

on voit, d'après le théorème relatif à la multiplication des déterminants, que le carré du déterminant des m formes linéaires $\xi^{(1)}, \ldots, \xi^{(m)}$ est égal à

$$(-1)^m U^2 \sum \pm \frac{\partial^2 \log U}{\partial u_1 \partial u_1} \cdots \frac{\partial^2 \log U}{\partial u_m \partial u_m}$$

et qu'il est par suite égal à une fonction entière à coefficients entiers de U ; on lui donne le nom de *discriminant de la forme* U. Une forme U, dont les coefficients sont des entiers rationnels sans diviseur commun, prend le nom de *forme primitive;* elle est une forme unité rationnelle.

Supposons qu'en particulier $\alpha_1, \ldots, \alpha_m$ forment une base d'un idéal $\mathfrak{a}$, la norme $n(\xi) = n(\alpha_1 u_1 + \ldots + \alpha_m u_m)$ est une forme décomposable de degré m. Les coefficients de cette forme sont des entiers dont le plus grand commun diviseur est $n(\mathfrak{a})$. Lorsqu'on supprime ce facteur on crée une forme U, à laquelle on donne le nom de *forme décomposable du corps k* et qui a les propriétés suivantes :

Si l'on remplace la base $\alpha_1, \ldots, \alpha_m$ par une autre base $\alpha_1^*, \ldots, \alpha_m^*$ du même idéal $\mathfrak{a}$ on obtient une nouvelle forme U^* qui se déduit de U par une transformation linéaire à coefficients entiers rationnels et dont le déterminant $= \pm 1$. Si l'on réunit toutes ces formes transformées dans le concept de *classes de forme*, on voit qu'à chaque idéal $\mathfrak{a}$ correspond une classe de formes. On obtient la même classe de formes en partant de $\alpha\mathfrak{a}$ au lieu de partir de $\mathfrak{a}$, α désignant un nombre quelconque entier ou fractionnaire du corps, c'est-à-dire qu'à chaque idéal d'une même classe correspond une même classe de formes.

Comme il est évident que le discriminant de la forme $n(\xi) = n(\mathfrak{a})U$ est égal à $n(\mathfrak{a})^2 d$, il en résulte :

Théorème 58. — Le discriminant d'une forme décomposable U du corps est égal au discriminant du corps. [Dedekind [1].]

Les propriétés des formes U que nous venons d'énoncer les déterminent complètement; car on a le théorème réciproque.

Théorème 59. — Soit U une forme primitive, décomposable dans k, mais indécomposable dans tout corps de dégré inférieur, de degré m et de discriminant d égal au discriminant du corps, nous pouvons affirmer qu'il y a dans k au moins une et au plus m classes d'idéaux auxquelles appartient cette forme U.

Démonstration. — Soit, par exemple,

$$\eta = \mu_1 u_1 + \ldots + \mu_m u_m$$

un facteur linéaire de U, dont les coefficients sont des nombres de k, nous multiplierons η par un nombre a tel que

$$\xi = a\eta = \alpha_1 u_1 + \ldots + \alpha_m u_m$$

soit une forme linéaire à coefficients entiers $\alpha_1, \ldots, \alpha_m$. Posons $\mathfrak{a} = (\alpha_1, \ldots, \alpha_m)$; on voit, d'après le théorème 20, que $n(\xi) = n(\mathfrak{a})U$, et comme le discriminant de la forme U est égal au discriminant du corps, on voit que

$$\begin{vmatrix} \alpha_1', & \ldots, & \alpha_m' \\ \cdot & \cdot & \cdot \\ \alpha_1^{(m-1)}, & \ldots, & \alpha_m^{(m-1)} \end{vmatrix}^2 = n(\mathfrak{a})^2 d.$$

Il résulte de là, grâce à la réciproque du théorème 19, que $\alpha_1, \ldots, \alpha_m$ forment la base de l'idéal $\mathfrak{a}$.

Si les deux formes U et V correspondent aux deux idéaux $\mathfrak{a}$ et $\mathfrak{b}$, la forme W, qui correspond à l'idéal $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$, est dite une *forme composée* de U et de V. [Dedekind[1].]

D'après ce qui vient d'être dit, reconnaître si deux formes données du corps k appartiennent ou non à la même classe, cela revient à reconnaître l'équivalence de deux idéaux donnés. Cette recherche n'exige qu'un nombre fini d'opérations. (Voir § 24.)

CHAPITRE IX.

Les anneaux du corps.

§ 31. — L'anneau. — L'idéal d'anneau et ses propriétés les plus importantes.

Soient $\theta, \eta, \ldots$ des nombres algébriques quelconques appartenant au domaine de rationnalité du corps k de degré m, on appellera *anneau de nombres, anneau* ou *domaine d'intégrité* le système formé par toutes les fonctions entières de $\theta, \eta, \ldots$ à coefficients entiers rationnels.

La somme, la différence, le produit de deux nombres de l'anneau donnent un nombre de l'anneau. Le concept d'anneau est donc invariant relativement à l'addition, la soustraction et la multiplication.

Le plus grand anneau du corps est celui que déterminent $\omega_1, \ldots \omega_m$ où $\omega_1, \ldots, \omega_m$ forment une base du corps. Tout anneau r contient m entiers $\rho_1, \ldots, \rho_m$ tels que tout autre nombre de l'anneau ρ puisse être mis sous la forme

$$\rho = a_1\rho_1 + \ldots + a_m\rho_m,$$

$a_1, \ldots, a_m$ étant des entiers rationnels. On dit que $\rho_1, \ldots, \rho_m$ forment une *base de l'anneau*. Désignons par $\rho_1', \ldots, \rho_m', \rho_1^{(m-1)}, \ldots, \rho_m^{(m-1)}$ les nombres conjugués de $\rho_1, \ldots, \rho_m$ le carré du déterminant

$$\begin{vmatrix} \rho_1, & \ldots, & \rho_m \\ \rho_1', & \ldots, & \rho_m' \\ \cdot & \cdot & \cdot \\ \rho_1^{(m-1)}, & \ldots, & \rho_m^{(m-1)} \end{vmatrix}$$

est un nombre rationnel et on le nomme le *discriminant de d_r de l'anneau r*.

Un *idéal d'anneau* ou un *idéal de l'anneau* r est un système illimité de nombres entiers algébriques $\alpha_1, \alpha_2, \ldots$ de l'anneau r qui a la propriété suivante : toute combinaison linéaire $\lambda_1\alpha_1 + \lambda_2\alpha_2 + \ldots$ appartient au système, les coefficients $\lambda_1, \lambda_2, \ldots$ étant des nombres quelconques de l'anneau r.

Tout idéal d'anneau contient m nombres entiers $i_1, \ldots, i_m$ telles que tout nombre de l'idéal d'anneau soit égal à une combinaison linéaire de la forme

$$a_1 i_1 + \ldots + a_m i_m$$

où $a_1, \ldots, a_m$ sont des entiers rationnels. Les nombres $i_1, \ldots, i_m$ forment une *base de l'idéal d'anneau.*

On démontre l'existence d'une base de l'anneau et celle d'une base de l'idéal d'anneau exactement comme on a démontré l'existence d'une base du corps et celle d'une base d'un idéal aux §§ 3 et 4.

On a les théorèmes suivants : [Dedekind [3].]

Théorème 60. — Soient $i_1, \ldots, i_m$ m entiers quelconques du corps k qui ne sont liés par aucune relation linéaire à coefficients entiers, il existe toujours un anneau r tel qu'en désignant par A un nombre entier rationnel convenablement choisi $Ai_1, \ldots, Ai_m$ formant la base d'un idéal de l'anneau.

Le théorème 60 se déduit du théorème suivant :

Théorème 61. — Il y a dans chaque anneau r des idéaux d'anneaux $\mathfrak{j}_r$ qui sont aussi des idéaux du corps.

Démonstration. — Exprimons $\omega_1, \ldots, \omega_m$ en fonction des m nombres de base $\rho_1, \ldots, \rho_m$ de l'anneau sous la forme

$$\omega_i = \frac{a_{i1}\rho_1 + \ldots + a_{im}\rho_m}{A} \qquad (i = 1, 2, \ldots, m)$$

où $a_{i1}, \ldots, a_{im}$ et A sont des entiers rationnels, il en résulte que tout entier du corps k divisible par A est un nombre de l'anneau et que par suite tout idéal du corps divisible par A est aussi un idéal de l'anneau r.

Le plus grand commun diviseur idéal de tous les idéaux du corps, qui sont aussi des idéaux de l'anneau r, est dit le *conducteur* $\mathfrak{f}$ *de l'anneau.* [Dedekind [3].] D'où :

Théorème 62. — Tout idéal $\mathfrak{j}$ du corps qui est divisible par le conducteur $\mathfrak{f}$ est aussi un idéal d'anneau de l'anneau r.

§ 32. — Les anneaux déterminés par un nombre entier. — Le théorème concernant la différente d'un nombre entier du corps.

Les anneaux les plus importants sont ceux qui sont déterminés par un seul nombre entier θ du corps. Dedekind a fondé sa théorie des discriminants des corps algébriques sur les propriétés de ces anneaux particuliers. [Dedekind [6].]

Nous résumerons les principaux résultats de Dedekind dans le théorème suivant :

Théorème 63. — Le plus grand commun diviseur des différentes de tous les entiers du corps k est égal à la différente $\mathfrak{d}$ du corps. Soit δ la différente d'un entier θ qui détermine le corps et $\mathfrak{f}$ le conducteur de l'anneau déterminé par θ, on a $\delta = \mathfrak{f}\theta$.

Démonstration. — Soit $\omega_1, \ldots, \omega_m$ une base de k et soient $\omega'_1, \ldots, \omega'_m, \omega_1^{(m-1)}, \ldots, \omega_m^{(m-1)}$ les nombres conjugués de ces m nombres. Formons le déterminant à m^2 termes $\omega_m^{(l)}$:

$$\Omega = \begin{vmatrix} \omega_1, & \ldots, & \omega_m \\ \omega'_1, & \ldots, & \omega'_m \\ \ldots & \ldots & \ldots \\ \omega_1^{(m-1)}, & \ldots, & \omega_m^{(m-1)} \end{vmatrix}$$

et désignons les mineurs relatifs à $\omega_1, \ldots, \omega_m$ par $\Omega_1, \ldots, \Omega_m$. Les m produits $\Omega\Omega_1, \ldots, \Omega\Omega_m$ sont alors m entiers du corps k et ils forment les nombres de base d'un idéal du corps k.

En effet, multiplions les $(m-1)$ lignes horizontales du déterminant Ω_h respectivement par

(16) $$u + \omega'_l, \quad u + \omega''_l, \quad \ldots, \quad u + \omega_l^{(m-1)}$$

où u est un paramètre indéterminé. Le déterminant à $m-1$ lignes prend alors la forme

$$f_1(u)\Omega_1 + f_2(u)\Omega_2 + \ldots + f_m(u)\Omega_m$$

où $f_1, \ldots, f_m$ sont des fonctions entières à coefficients entiers de u.

D'autre part, le produit des $m-1$ facteurs linéaires (16) est

$$u^{(m-1)} + (\omega'_l + \ldots + \omega_l^{(m-1)})u^{m-2} + \ldots = u^{m-1} + (a - \omega_l)u^{m-2} + \ldots$$

où a est un entier rationnel. Si l'on compare les coefficients de u^{m-2}, on voit que $\omega_l\Omega_h$ est une combinaison linéaire à coefficients entiers rationnels de $\Omega_1, \ldots, \Omega_m$, ce qui démontre que $\Omega\Omega_1, \ldots, \Omega\Omega_m$ sont les nombres de bases d'un idéal.

Soit $\Omega_h^{(l)}$ le déterminant mineur relatif à $\omega_h^{(l)}$, on sait que le déterminant à m lignes formé par les Ω_h^l est égal à Ω^{m-1}; par suite, la norme de l'idéal $\mathfrak{J} = (\Omega\Omega_1, \ldots, \Omega\Omega_m)$ satisfait à

$$dn^2(\mathfrak{J}) = |\Omega\Omega_h^{(l)}|^2 = \Omega^{2m-2},$$

et par suite $n(\mathfrak{J}) = |d|^{m-1}$. Mais il est évident que le déterminant d du corps est divisible par $\mathfrak{J}$; posons $d = \mathfrak{J}\mathfrak{j}$, il en résulte que $n(\mathfrak{j}) = |d|$.

Soit θ un nombre quelconque qui détermine le corps; nous pouvons mettre les m nombres de base du corps sous la forme

$$\omega_1 = 1,$$
$$\omega_2 = \frac{a_1 + \theta}{f_1},$$
$$\omega_3 = \frac{a_2 + a'_2\theta + \theta^2}{f_2},$$
$$\ldots\ldots\ldots\ldots$$
$$\omega_m = \frac{a_{m-1} + a'_{m-1}\theta + \ldots + a_{m-1}^{(m-2)}\theta^{m-2} + \theta^{m-1}}{f_{m-1}}$$

où $a_1, a_2, a'_2, \ldots, a_{m-1}^{(m-2)}, f_1, \ldots, f_{m-1}$ sont des nombres entiers rationnels.

Déterminons maintenant le conducteur $\mathfrak{f}$ de l'anneau déterminé par θ et nous mettrons les nombres de base sous la forme

$$\rho_1 = f'_1,$$
$$\rho_2 = b_1 + f'_2\theta,$$
$$\rho_3 = b_2 + b'_2\theta + f'_3\theta^2,$$
$$\ldots\ldots\ldots\ldots$$
$$\rho_m = b_{m-1} + b'_{m-1}\theta + \ldots + b_{m-1}^{(m-2)}\theta^{m-2} + f'_m\theta^{m-1},$$

$b_1, b_2, \ldots, b_{m-1}, f'_1, f'_2, \ldots, f'_m$ étant des entiers rationnels.

D'après le théorème 62, $\rho_1\omega_m, \rho_2\omega_{m-1}, \ldots, \rho_m\omega_1$ ne peuvent être que des fonctions entières à coefficients entiers de θ; il en résulte nécessairement que f'_1 est divisible par f_{m-1}, f'_2 l'est par $f_{m-2}, \ldots, f'_{m-1}$ par f_1 et par suite le produit $f'_1, \ldots, f'_{m-1}$ est divisible par le produit $f = f_1 \ldots f_{m-1}$. Mais comme $n(\mathfrak{f}) = f_1 \ldots f_{m-1} f'_1 \ldots f'_{m-1} f'_m$, on a

$$n(\mathfrak{f}) = f^2 g$$

où g est un entier rationnel.

Posons, de plus,

$$\Theta = \begin{vmatrix} 1, & \theta, & \ldots, & \theta^{m-1} \\ 1, & \theta', & \ldots, & \theta'^{m-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1, & \theta^{(m-1)}, & \ldots, & (\theta^{(m-1)})^{m-1} \end{vmatrix}, \qquad H = (-1)^{\frac{m-1}{2}} \begin{vmatrix} 1, & \theta', & \ldots, & \theta'^{m-2} \\ \ldots & \ldots & \ldots & \ldots \\ 1, & \theta^{(m-1)}, & \ldots, & (\theta^{(m-1)})^{m-2} \end{vmatrix}.$$

On a alors pour la différente δ du nombre θ

$$(-1)^{m-1}\delta = \frac{\Theta}{H};$$

et, d'après ce qui a été dit au début,

$$(-1)^{\frac{m(m-1)}{2}} n(\delta) = \Theta^2 = f^2 d,$$

$$(17)\qquad \sum_{(h=1,2,\ldots,m)} u_h \Omega_h = \frac{\Theta}{f^2} \begin{vmatrix} u_1, & f_1 u_2, & f_2 u_3, & \ldots, & f_{m-1} u_m \\ 1, & a_1 + \theta', & a_2 + a'_2\theta' + \theta'^2, & \ldots, & a_{m-1} + \ldots + \theta'^{m-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 1, & a_1 + \theta^{(m-1)}, & a_2 + a'_2\theta^{(m-1)} + (\theta^{(m-1)})^2, & \ldots, & a_{m-1} + \ldots + (\theta^{(m-1)})^{m-1} \end{vmatrix}$$

où $u_1, \ldots, u_m$ sont des indéterminées. Développons ce déterminant suivant les éléments de la première ligne, il s'écrira

$$u_1 \mathrm{H}_1 + \ldots + u_m \mathrm{H}_m.$$

Il est facile de voir que $\frac{\mathrm{H}_1}{\mathrm{H}}, \ldots, \frac{\mathrm{H}_m}{\mathrm{H}}$ sont alors tous des nombres entiers du corps k; ils s'obtiennent, comme le montre la formule 17, en multipliant les nombres $\Omega_1, \ldots, \Omega_m$ par un seul et même facteur situé dans k. Les m nombres $\frac{\mathrm{H}_1}{\mathrm{H}}, \ldots, \frac{\mathrm{H}_m}{\mathrm{H}}$ sont encore les bases d'un idéal; soit $\mathfrak{m}$ cet idéal.

Les nombres de l'idéal $\mathfrak{m}$ sont tous des fonctions entières à coefficients entiers de θ; cet idéal est donc divisible par $\mathfrak{f}$. Posons $\mathfrak{m} = \mathfrak{f}\mathfrak{l}$ où $\mathfrak{l}$ est un idéal dans k. Notre équation (17) montre alors que

$$\mathfrak{J} = \frac{\Theta \mathrm{H}}{f^2} \mathfrak{f}\mathfrak{l} = \frac{d\mathfrak{f}\mathfrak{l}}{\delta};$$

d'où, en prenant la norme, il résulte

$$|d|^{m-1} = \frac{|d|^m n(\mathfrak{f}) n(\mathfrak{l})}{f^2 |d|}, \qquad \text{c'est-à-dire} \qquad f^2 = n(\mathfrak{f}) n(\mathfrak{l});$$

comme d'autre part on a trouvé $n(\mathfrak{f}) = f^2 g$, il faut que $g = 1$, $n(\mathfrak{l}) = 1$ et par suite $n(\mathfrak{f}) = f^2$, $\mathfrak{J}\delta = \mathfrak{f}d$, $\delta = \mathfrak{f}\mathfrak{j}$.

Soit maintenant $\mathfrak{p}$ un idéal premier donné du corps k; nous démontrerons tout d'abord que l'on peut toujours trouver dans k un nombre $\theta = \rho$ tel que le conducteur de l'anneau déterminé par ρ ne soit pas divisible par $\mathfrak{p}$. Soit p le nombre premier rationnel divisible par $\mathfrak{p}$, $p = \mathfrak{p}^e \mathfrak{a}$ où $\mathfrak{a}$ est un idéal premier avec $\mathfrak{p}$; de plus, soit ρ un entier de k, choisi de telle sorte que tout nombre entier de k soit congru à une fonction entière à coefficients entiers de ρ suivant toute puissance de $\mathfrak{p}$. Le théorème 29 montre l'existence d'un pareil nombre; de plus, supposons $\rho \equiv 0$ suivant $\mathfrak{a}$ (théorème 25) et que ρ soit un nombre qui détermine le corps. Supposons que le descriminant de $\rho = p^h a$ où a est un entier rationnel premier avec p.

Tout nombre entier ω du corps peut alors être mis sous la forme

$$\omega = \frac{F(\rho)}{a\rho^h}$$

où $F(\rho)$ est une fonction entière à coefficients entiers de ρ.

En effet, si $\omega \equiv H(\rho)$ suivant $\mathfrak{p}^{eh}$ où $H(\rho)$ est une fonction entière à coefficients entiers de ρ, posons $\omega = H(\rho) + \omega^*$, il en résulte que $\omega^* \rho^h$ est divisible par p^h. Posons $\omega^* \rho^h = p^h \alpha$ où α est un entier du corps k. Comme d'après le § 3 tout nombre entier α peut être mis sous la forme $\frac{G(\rho)}{d(\rho)}$ où $G(\rho)$ est une fonction entière à coefficients entiers de ρ, il en résulte $\omega^* = \frac{G(\rho)}{a\rho^h}$ et de plus

$$\omega = \frac{a\rho^h H(\rho) + G(\rho)}{a\rho^h}.$$

Cette propriété de ρ que nous venons de trouver nous montre que le nombre $a\rho^h$ se trouve certainement dans le conducteur $\mathfrak{f}$ de l'anneau déterminé par ρ. $\mathfrak{f}$ n'est donc pas divisible par $\mathfrak{p}$, c'est-à-dire que $\rho = \theta$ est un nombre répondant aux conditions indiquées.

Ces derniers développements prouvent que $\mathfrak{j}$ est exactement le plus grand commun diviseur des différentes de tous les nombres entiers. D'autre part, ce plus grand commun diviseur, comme il résulte de la définition de la différente du corps $\mathfrak{d}$, contient nécessairement cet idéal $\mathfrak{d}$ en facteur; nous poserons $\mathfrak{j} = \mathfrak{h}\mathfrak{d}$. Comme suivant le théorème 13 $n(\mathfrak{d})$ est divisible par le discriminant d, il en résulte que $n(\mathfrak{j}) = n(\mathfrak{h})da$ où a est un entier rationnel. Mais comme $n(\mathfrak{j}) = \pm d$, il en résulte $n(\mathfrak{h}) = 1$, $\mathfrak{h} = 1$, $a = \pm 1$.

Du théorème 63 on déduit facilement les théorèmes 31 et 37, ainsi que les affirmations énoncées à la fin du § 12 relatives aux nombres premiers contenus dans le discriminant du corps. Il suffit pour déduire ces dernières de décomposer le premier membre de l'équation à laquelle satisfait $\theta = \rho$ suivant le nombre premier en question p, et de raisonner comme il a été fait au § 11, pour le premier membre de l'équation fondamentale.

§ 33. — Les idéaux d'anneaux réguliers et leurs lois de divisibilité.

Soit r un anneau quelconque et $\mathfrak{j}_r = [\alpha_1, \ldots, \alpha_s]$ un idéal d'anneau de r, le plus grand commun diviseur des nombres de ce dernier est un idéal du corps; nous nommerons cet idéal $\mathfrak{j} = (\alpha_1, \ldots, \alpha_s)$ l'*idéal du corps correspondant à* $\mathfrak{j}_r$.

Lorsqu'en particulier l'idéal du corps $\mathfrak{j}$ est premier avec le conducteur $\mathfrak{f}$ de l'anneau r, nous dirons que $\mathfrak{j}_r$ est un *idéal d'anneau régulier*.

Théorème. — Soit $\mathfrak{j}$ un idéal du corps premier avec le conducteur $\mathfrak{f}$, il y a toujours dans l'anneau r un idéal d'anneau $\mathfrak{j}_r$ auquel correspond l'idéal du corps $\mathfrak{j}$.

Démonstration. — Déterminons le système de tous les nombres de l'anneau r, qui sont divisibles par l'idéal donné $\mathfrak{j}$ du corps. Ces nombres forment dans r un idéal d'anneau $\mathfrak{j}_r = (\alpha_1, \ldots, \alpha_s)$. Ensuite nous choisissons dans le conducteur $\mathfrak{f}$ de l'anneau un nombre entier φ premier avec $\mathfrak{j}$ et dans $\mathfrak{j}$ un nombre α premier avec φ. Il existera dès lors deux nombres entiers du corps ψ et β tels que $\varphi\psi + \alpha\beta = 1$.

Comme $\varphi\psi$ est divisible par $\mathfrak{f}$ et qu'il fait partie de l'anneau r, $\alpha\beta$ est aussi un nombre de l'anneau r, et comme d'autre part $\alpha\beta$ est divisible par $\mathfrak{j}$, $\alpha\beta = 1 - \varphi\psi$ est un nombre de l'anneau $\mathfrak{j}_r$; et par suite l'idéal du coprs $\mathfrak{j}^* = (\alpha_1, \ldots, \alpha_s)$ est premier avec $\mathfrak{f}$.

Comme $\mathfrak{j}^*$ est divisible par $\mathfrak{j}$ et qu'il divise le produit $\mathfrak{f}\mathfrak{j}$, il en résulte que $\mathfrak{j}^* = \mathfrak{j}$, c'est-à-dire que $\mathfrak{j}_r$ est un idéal d'anneau régulier auquel correspond l'idéal du corps $\mathfrak{j}$, ce qui démontre le théorème 64.

On entend par *produit de deux idéaux d'anneaux*

$$\mathfrak{a}_r = [\alpha_1, \ldots, \alpha_s] \quad \text{et} \quad \mathfrak{b}_r = [\beta_1, \ldots, \beta_t]$$

l'idéal d'anneau

$$\mathfrak{a}_r\mathfrak{b}_r = [\alpha_1\beta_1, \ldots, \alpha_s\beta_1, \ldots, \alpha_1\beta_t, \ldots, \alpha_s\beta_t].$$

Il en résulte évidemment le

Théorème 65. — Au produit de deux idéaux d'anneau réguliers correspond toujours le produit des idéaux du corps qui correspondent aux facteurs.

Par suite de ce théorème, les lois de divisibilité et de décomposition des idéaux d'anneau réguliers coïncident avec les lois de divisibilité et de décomposition des idéaux du corps premiers avec $\mathfrak{f}$.

Dans ce qui suit, nous ne nous occuperons que d'idéaux d'anneau réguliers, nous n'ajouterons plus le mot régulier, c'est-à-dire que lorsque nous parlerons d'*un idéal d'anneau* il sera sous-entendu qu'il est régulier.

Le théorème 23 nous apprend qu'il existe toujours dans le corps k $\varphi(\mathfrak{f})$ nombres entiers incongrus suivant l'idéal $\mathfrak{f}$ et premier avec $\mathfrak{f}$. Lorsque l'un de ces nombres appartient à l'anneau r, cet anneau contient évidemment tous les nombres congrus à celui-ci suivant le conducteur $\mathfrak{f}$. Le nombre des entiers incongrus suivant $\mathfrak{f}$ et premiers avec $\mathfrak{f}$ contenu dans r est un diviseur de $\varphi(\mathfrak{f})$; nous le désignerons par $\varphi_r(\mathfrak{f})$.

La *norme* $n(\mathfrak{a}_r)$ *d'un idéal d'anneau* $\mathfrak{a}_r$ n'est autre chose que la norme de l'idéal du corps $\mathfrak{a}$ qui correspond à $\mathfrak{a}_r$. Cette définition nous donne les propositions élémentaires relative aux normes des idéaux d'anneau.

§ 34. — Les unités d'un anneau. — Les classes d'un anneau.

Le théorème relatif à l'existence des unités fondamentales se retrouve dans un anneau; la manière la plus simple de le déduire du théorème démontré pour les unités du corps consiste à remarquer qu'il résulte du théorème 24 que toute puissance $\varphi(\mathfrak{f})^{\text{ème}}$ d'une unité du corps nous donne une unité de l'anneau. Le théorème 47, vrai pour les unités du corps, peut s'énoncer sous la même forme. Désignons ici par s le nombre que nous avons désigné par r au théorème 47. Soient $\varepsilon_1, \ldots, \varepsilon_s$ un système d'unités fondamentales de l'anneau, c'est-à-dire un système de s unités dans l'anneau r tel que toutes les unités de r puissent s'exprimer au moyen du produit de ces nombres et des racines de l'unité contenues dans l'anneau. Nous appellerons régulateur R_r de l'anneau le déterminant des s premiers logarithmes de ces unités pris positivement. Nous désignerons par w_r le nombre des racines de l'unité situées dans r. [Dedekind[3].]

Deux idéaux d'anneau $\mathfrak{a}$ et $\mathfrak{b}$ seront dits équivalents, s'il existe deux entiers μ et λ tels que $\mu\mathfrak{a} = \lambda\mathfrak{b}$. Ici nous considérerons le concept d'équivalence dans le sens restreint, c'est-à-dire que nous ferons la réserve suivante : la norme de $\frac{\mu}{\lambda}$ est positive.

Tous les idéaux d'anneau équivalents forment *une classe de l'anneau*. Un idéal d'anneau (α) où α est un nombre entier positif premier avec $\mathfrak{f}$ est dit un idéal d'anneau principal; sa classe est dite *une classe principale de l'anneau*. Les autres définitions et les théorèmes relatifs à la multiplication des classes d'un anneau correspondent exactement à ce que nous avons établi aux §§ 22, 28, 29 pour les classes d'idéaux d'un corps; on voit, comme au § 22, que le nombre des classes d'un anneau est limité.

On peut employer pour déterminer le nombre des classes deux méthodes : soit des moyens purement arithmétiques, soit la voie analytique, comme il a été indiqué aux §§ 25 et 26. On obtient le résultat suivant : [Dedekind[3].]

Théorème 66. — Soit h et h_r le nombre des classes d'idéaux du corps et de l'anneau r, tous deux dans le sens restreint du concept de classes, on a

$$\frac{h_r}{h} = \frac{\varphi(\mathfrak{f})\, w\, R_r}{\varphi_r(\mathfrak{f})\, w_r\, R}.$$

Les formations du chapitre VIII se retrouvent dans l'anneau, et l'on peut parvenir ainsi à la notion de *forme décomposable* correspondant à une classe d'un anneau.

§ 35. — Le module. — La classe de module.

Soient $\mu_1, \ldots, \mu_m$ m nombres entiers du corps k qui ne sont liés par aucune relation linéaire et homogène à coefficients entiers rationnels, le système des nombres de la forme $a_1\mu_1 + \ldots + a_m\mu_m$ où $a_1, \ldots, a_m$ sont des entiers rationnels est dit un *module du corps k*, et on l'écrit $[\mu_1, \ldots, \mu_m]$. Le concept de module est un invariant pour l'addition et la soustraction. On a des exemples de modules : le système de tous les entiers du corps k, un idéal, un anneau, un idéal d'anneau. Deux modules $[\mu_1, \ldots, \mu_m]$ et $[\lambda_1, \ldots; \lambda_m]$ sont dits *équivalents* lorsqu'il existe deux entiers, μ et λ, tels que $[\mu\mu_1, \ldots, \mu\mu_m] = [\lambda\lambda_1, \ldots, \lambda\lambda_m]$. Tous les modules équivalents entre eux forment une *classe de modules*. Dedekind a pris le concept de module comme base de ses recherches sur les nombres algébriques. [Dedekind[1, 3, 6, 9].]

Le carré du déterminant

$$\begin{vmatrix} \mu_1, & \ldots, & \mu_m \\ \mu'_1, & \ldots, & \mu'_m \\ \cdots & \cdots & \cdots \\ \mu_1^{(m-1)}, & \ldots, & \mu_m^{(m-1)} \end{vmatrix}$$

est, on le voit facilement, un nombre entier rationnel, divisible par le carré de la norme de l'idéal $\mathfrak{m} = (\mu_1, \ldots, \mu_m)$. On désigne par ∂ le quotient de ces deux carrés. On retrouve la même valeur ∂ si l'on forme le même quotient pour tout module équivalent à $[\mu_1, \ldots, \mu_m]$. Le nombre entier rationnel ∂ caractérise par conséquent la classe de modules déterminée par $[\mu_1, \ldots, \mu_m]$; on lui donne le nom de *discriminant de la classe de modules*.

Les concepts de *forme décomposable* et de *classe de formes* pour le module se définissent d'une façon analogue à celle que nous avons donnée au § 30 pour le corps. [Dedekind[3].]

Toulouse. - Imprimerie et Librairie Édouard Privat, rue des Arts, 14. — 853.

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

MÉMOIRE de M. David Hilbert,
Professeur à l'Université de Gœttingen.

PUBLIÉ PAR LA SOCIÉTÉ
DEUTSCHE MATHEMATIKER VEREINIGUNG, en 1897.

Traduit par M. A. Levy,
Professeur au Lycée Saint-Louis.

DEUXIÈME PARTIE.

LE CORPS DES NOMBRES DE GALOIS.

CHAPITRE X.

Les idéaux premiers du corps de Galois et de ses sous-corps.

§ 36. — La décomposition unique des idéaux du corps de Galois en idéaux premiers.

Un corps K qui coïncide avec tous ses corps conjugués est dit un *corps de Galois*. Soit k un corps quelconque de degré m et soit $k', \ldots, k^{(m-1)}$ les m corps conjugués à k, on peut, en réunissant tous les nombres appartenant aux corps $k, k', \ldots, k^{(m-1)}$, former un nouveau corps K; ce corps K est alors nécessairement un corps de Galois, qui contient les corps $k, k', \ldots, k^{(m-1)}$ comme sous-corps. Tout corps k peut donc être considéré comme un sous-corps d'un corps de Galois. Par suite de cette circonstance nous n'apporterions aucune restriction essentielle à l'étude des nombres algébriques si nous commencions par étudier un corps de Galois, et si nous cherchions à voir ensuite comment les lois de décomposition des idéaux de ce corps de Galois se modifient lorsqu'on passe à un des sous-corps qu'il contient.

La démonstration de la décomposition unique des idéaux en idéaux premiers est très simple pour un corps de Galois [Hilbert[12]]. Pour le voir, nous fixerons d'abord le sens de certaines notations.

Soit Θ le nombre entier qui détermine le corps K de degré M; Θ est une racine d'une équation irréductible de degré M à coefficients entiers et rationnels. Désignons les M racines de cette équation par

$$s_1\Theta = \Theta, \quad s_2\Theta, \quad \ldots, \quad s_M\Theta,$$

où $s_1, \ldots, s_M$ désignent des fonctions rationnelles de Θ à coefficients rationnels. Si l'on considère $s_1\Theta, \ldots, s_M\Theta$ comme des substitutions, elles forment un groupe G de degré M, car deux substitutions successives prises parmi ces M nous donnent encore une de ces substitutions. Soit G le *groupe du corps de Galois* K. Un idéal $\mathfrak{J}$ qui ne change pas lorsqu'on y remplace ses nombres par leurs conjugués, c'est-à-dire lorsqu'on fait les M — 1 substitutions $s_2, \ldots, s_M$ sera dit un *Idéal invariant*. Un idéal invariant a les propriétés suivantes :

LEMME 11. — La puissance $M!^{\text{ème}}$ de tout idéal invariant $\mathfrak{J}$ est un nombre entier rationnel.

Démonstration. — Soit A un nombre de l'idéal $\mathfrak{J}$ et soient $A_1, A_2, \ldots, A_M$ les M fonctions symétriques élémentaires des nombres $A = s_1 A, s_2 A, \ldots, s_M A$. Nous désignerons par $\bar{A}$ le plus grand commun diviseur des M nombres rationnels entiers

$$(18) \qquad A_1^{\frac{M!}{1}}, \quad A_2^{\frac{M!}{2}}, \quad \ldots, \quad A_M^{\frac{M!}{M}}.$$

De même supposons qu'on ait calculé les mêmes fonctions symétriques et le même plus grand commun diviseur relatifs à tous les nombres B, Γ, ..., de l'idéal $\mathfrak{J}$ et soient $\bar{B}, \bar{C}, \ldots$ ces diviseurs.

Soit J le plus grand commun diviseur de tous les nombres $\bar{A}, \bar{B}, \bar{C}, \ldots$ ainsi obtenus.

On a

$$\mathfrak{J}^{M!} = J.$$

En effet, les nombres conjugués à A étant aussi des nombres de $\mathfrak{J}$, on a

$$A_1 \equiv 0, (\mathfrak{J}), \quad A_2 \equiv 0, (\mathfrak{J}^2), \quad \ldots, \quad A_M \equiv 0, (\mathfrak{J}^M),$$

et par suite tous les nombres (18) et de plus $\bar{A}$ sont $\equiv 0, (\mathfrak{J}^{M!})$.

Comme on peut en dire autant de $\bar{B}, \bar{C}, \ldots$, on a aussi $J \equiv 0$ d'après $\mathfrak{J}^{M!}$.

D'autre part, les coefficients $A_1, A_2, \ldots, A_M$ de l'équation de degré M en A sont divisibles respectivement par $J^{\frac{1}{M!}}, \ldots, J^{\frac{M}{M!}}$ et par suite A est divisible par $J^{\frac{1}{M!}}$; comme on peut en dire autant de tous les nombres B, Γ, ... de l'idéal $\mathfrak{J}$, il en résulte que $\mathfrak{J}^{M!}$ est divisible par J.

Théorème 67. — A chaque idéal $\mathfrak{A}$ du corps de Galois K on peut faire correspondre un autre idéal $\mathfrak{B}$, tel que le produit $\mathfrak{A}\mathfrak{B}$ soit un idéal principal.

Démonstration. — L'idéal $\mathfrak{J} = \mathfrak{A} s_2\mathfrak{A} \ldots\ldots s_M\mathfrak{A}$ est un idéal invariant, donc, d'après le lemme 11, l'idéal

$$\mathfrak{B} = \mathfrak{J}^{M-1} s_2\mathfrak{A} \ldots\ldots s_M\mathfrak{A}$$

est l'idéal indiqué au théorème 67.

Ce théorème 67 permet de développer les caractères de divisibilité dans un corps de Galois, comme on l'a fait au paragraphe 5 en vertu du théorème 8 pour un corps quelconque k.

Pour déduire alors des lois de divisibilité dans un corps de Galois, les lois de divisibilité pour un corps quelconque k, il faudra démontrer d'abord dans un corps de Galois les théorèmes de Kronecker 13 et 14 relatifs aux formes et on en conclura l'exactitude de ces lois pour un sous-corps k, ou bien on emploiera un moyen direct et approprié de transposition d'un corps à l'autre. [Hilbert[2].]

§ 37. — Les éléments, la différente et le discriminant du corps de Galois.

Certaines notions établies antérieurement prennent un sens plus simple dans le corps de Galois. Ainsi les éléments d'un corps de Galois sont des idéaux dans le corps lui-même et on a les faits suivants :

Théorème 68. — Les éléments d'un corps de Galois K se transforment les uns dans les autres par les substitutions $s_1, \ldots, s_M$. La différente $\mathfrak{D}$ du corps K est un idéal invariant, et le discriminant $D = \pm N(\mathfrak{D})$ est comme idéal la M^e^ puissance de $\mathfrak{D}$.

Démonstration. — Désignons par $\Omega_1, \ldots, \Omega_M$ une base du corps K, les éléments de K sont des idéaux de la forme

$$\mathfrak{E}_2 = (\Omega_1 - s_2\Omega_1, \ \ldots, \ \Omega_M - s_2\Omega_M),$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$\mathfrak{E}_M = (\Omega_1 - s_M\Omega_1, \ \ldots, \ \Omega_M - s_M\Omega_M).$$

Appliquons une substitution quelconque s à l'un de ces éléments $\mathfrak{E}_i$ et remarquons que les nombres $s\Omega_1, \ldots, s\Omega_M$ forment encore une base du corps; il en résulte que si l'on pose $ss_i = s_{i'}s$:

$$s\mathfrak{E}_i = (s\Omega_1 - s_{i'}s\Omega_1, \ \ldots, \ s\Omega_M - s_{i'}s\Omega_M) = \mathfrak{E}_{i'}.$$

L'invariance de la différente du corps résulte de sa représentation

$$\mathfrak{D} = \mathfrak{E}_2 \ldots\ldots \mathfrak{E}_M.$$

§ 38. — Les sous-corps du corps de Galois.

Le corps de Galois permet une étude précise des lois de décomposition de ses nombres en tenant compte des sous-corps qu'il contient, et les résultats qu'on obtient ainsi sont très importants lorsqu'on veut appliquer la théorie générale des corps à des corps algébriques particuliers. [Hilbert[3].]

Pour caractériser simplement un sous-corps du corps de Galois, nous emploierons les expressions suivantes : Lorsque r substitutions $s_1 = 1, s_2, \ldots, s_r$ du groupe G forment un sous-groupe g de degré r, l'ensemble des nombres de K qui ne changent pas lorsqu'on applique toutes ces substitutions g, forme un corps contenu dans K et de degré $m = \frac{M}{r}$. Nous nommerons ce corps k le *sous-corps correspondant au sous-groupe* g.

Le corps de Galois appartient au groupe formé par $s_1 = 1$; au groupe G des M substitutions s correspond le corps des nombres rationnels. — Réciproquement, chaque sous-corps k du corps de Galois appartient à un certain sous-groupe g du groupe G. Le groupe g s'appelle alors le *sous-groupe qui détermine le corps* k.

§ 39. — Les corps de décomposition et le corps d'inertie d'un idéal premier $\mathfrak{P}$.

Choisissons dans le corps de Galois K un certain idéal premier $\mathfrak{P}$ de degré f; il y a un certain nombre de sous-corps de K s'emboîtant les uns dans les autres, caractérisés par l'idéal premier $\mathfrak{P}$ et dont nous allons développer brièvement les merveilleuses propriétés.

Soit p le nombre premier rationnel divisible par $\mathfrak{P}$; de plus, soient $z, z', z'', \ldots,$ les r_z substitutions du groupe G qui laissent invariable l'idéal premier $\mathfrak{P}$; elles forment un groupe de degré r_z que nous nommerons le *groupe de décomposition de l'idéal premier* $\mathfrak{P}$ et que nous désignerons par g_z. Le corps k_z correspondant au groupe g_z sera dit *le corps de décomposition de l'idéal premier* $\mathfrak{P}$; il est de degré $m = \frac{M}{r_z}$.

De plus, soient $t, t', t'', \ldots$ toutes les substitutions s du corps telles que pour tout nombre entier Ω du corps K on ait $s\Omega = \Omega$ suivant $\mathfrak{P}$ et soit r_t leur nombre, on voit facilement que ces substitutions forment un groupe de degré r_t. Ce groupe, nous le nommerons le *groupe d'inertie de l'idéal premier* $\mathfrak{P}$ et nous le désignerons par g_t. Le corps k_t qui correspond à g_t nous le désignerons par *corps d'inertie de l'idéal premier* $\mathfrak{P}$: il est de degré $m_t = \frac{M}{r_t}$.

Le rapport entre le groupe d'inertie et le groupe de décomposition résulte des faits suivants :

Théorème 69. — Le sous-groupe d'inertie g_t de l'idéal premier $\mathfrak{P}$ est un sous-groupe invariant du groupe de décomposition g_z. On obtient toutes les substitutions du groupe de décomposition et on n'obtient qu'une fois chacune d'elles en multipliant les substitutions du groupe d'inertie par $1, z, z^2, \ldots, z^{f-1}$, où z est une substitution appropriée du groupe de décomposition.

Démonstration. — Soit t une substitution quelconque de g_t et Ω un nombre entier du corps K divisible par $\mathfrak{P}$. Posons $\Omega' \equiv t^{-1}\Omega$; on a, en vertu de la propriété du corps d'inertie $\Omega' \equiv t\Omega' \equiv \Omega$ suivant $\mathfrak{P}$, c'est-à-dire $\Omega' \equiv 0$ suivant $\mathfrak{P}$. L'application de la substitution t donne $\Omega \equiv 0$ suivant l'idéal premier $t\mathfrak{P}$. Comme ceci a lieu pour tous les nombres Ω de l'idéal premier $\mathfrak{P}$, il faut que $\mathfrak{P}$ soit divisible par $t\mathfrak{P}$ et, par suite, $\mathfrak{P} = t\mathfrak{P}$, c'est-à-dire que le groupe d'inertie est un sous-groupe du groupe de décomposition.

Désignons maintenant par P un nombre primitif de l'idéal premier $\mathfrak{P}$ congru à 0 suivant tous les idéaux conjugués à $\mathfrak{P}$ et premiers avec $\mathfrak{P}$. Le théorème 25 montre que l'on peut former un pareil nombre. Ceci fait, composons la fonction entière à coefficients entiers de degré M en x :

$$\mathrm{F}(x) = (x - s_1\mathrm{P})(x - s_2\mathrm{P}) \ldots (x - s_{\mathrm{M}}\mathrm{P}).$$

Comme P est une racine entière de la congruence $\mathrm{F}(x) \equiv 0$ suivant $\mathfrak{P}$, on sait, d'après le théorème 27, que P^p est aussi racine de cette congruence, et il résulte de là que, parmi les M substitutions, l'une au moins donne $s\mathrm{P} \equiv \mathrm{P}^p$ suivant $\mathfrak{P}$. Si alors on avait $s^{-1}\mathfrak{P} \neq \mathfrak{P}$, on aurait, en vertu du choix de P, la congruence $\mathrm{P} \equiv 0$ suivant $s^{-1}\mathfrak{P}$, et, par suite, $s\mathrm{P} \equiv 0$ suivant $\mathfrak{P}$, ce qui est contraire à la congruence trouvée précédemment.

A cause de $s\mathfrak{P} = \mathfrak{P}$ la substitution s appartient au groupe de décomposition : posons $s = z$; en appliquant plusieurs fois de suite la substitution z à la congruence $z\mathrm{P} \equiv \mathrm{P}^p$ suivant $\mathfrak{P}$, nous aurons

$$z^2\mathrm{P} \equiv \mathrm{P}^{p^2}, \quad z^3\mathrm{P} \equiv \mathrm{P}^{p^3}, \quad \ldots, \quad z^f\mathrm{P} \equiv \mathrm{P}^{p^f} \equiv \mathrm{P} \quad (\text{suivant } \mathfrak{P}) ;$$

c'est pourquoi z^f est une substitution du groupe d'inertie, car tout nombre entier du corps Ω du corps K peut être mis sous la forme de $\Omega \equiv \mathrm{P}^a + \Pi$ ou $\equiv \Pi$, où a est un nombre entier rationnel et Π un nombre du corps divisible par $\mathfrak{P}$. A cause de $z^f\mathfrak{P} = \mathfrak{P}$ on a en effet $z^f\Omega \equiv \Omega$ suivant $\mathfrak{P}$.

La congruence $z\mathrm{P} \equiv \mathrm{P}^p$ suivant $\mathfrak{P}$ nous apprend que $z^{-1}tz\mathrm{P} \equiv \mathrm{P}$ suivant $\mathfrak{P}$, où t est une substitution quelconque du groupe d'inertie g_t. Si nous posons $z' = z^{-1}tz$ et si Ω est un nombre entier du corps tel que $\Omega \equiv \mathrm{P}^a$ suivant $(\mathfrak{P})$, $z'\Omega \equiv (z'\mathrm{P})^a \equiv \mathrm{P}^a \equiv \Omega$ suivant $\mathfrak{P}$, et de même si $\Omega \equiv 0$ suivant $\mathfrak{P}$, c'est-à-dire que $z' = z^{-1}tz$ appartient au groupe d'inertie.

Soit donc $P(\mathsf{P})$ la fonction entière à coefficients entiers de degré f de P qui $\equiv 0$ suivant $\mathfrak{P}$; alors, d'après le théorème 27, la congruence $P(x) \equiv 0$ suivant $\mathfrak{P}$ admet les racines $P, P^p, P^{p^{f-1}}$, et d'après le théorème 26 elle n'en a pas d'autres.

Soit maintenant z^* une substitution quelconque du groupe de décomposition; il résulte de la congruence $P(\mathsf{P}) \equiv 0$ suivant $\mathfrak{P}$, que $P(z^*P) \equiv 0$, et, par suite, $z^*P \equiv P^{p^i}$ suivant $\mathfrak{P}$, où i a l'une des f valeurs $0, 1, \dots, f-1$. Comme d'autre part $P^{p^i} \equiv z^iP$, $z^{-i}z^*P \equiv P$ suivant $\mathfrak{P}$, et, par suite, $z^{-i}z^*$ est une substitution t du groupe d'inertie, c'est-à-dire $z^* = z^it$.

Toutes les substitutions du groupe de décomposition peuvent donc être représentées sous cette forme, et comme réciproquement z^it pour $i = 0, 1, \dots, f-1$ représente des substitutions distinctes, la dernière partie du théorème 69 est démontrée. Enfin, l'invariance du groupe d'inertie résulte de ce fait que $z^{-1}tz$ appartient à ce groupe. De plus, on a $r_z = fr_t$.

§ 40. — Un théorème relatif au corps de décomposition.

Le théorème suivant exprime la propriété la plus importante du corps de décomposition.

Théorème 70. — L'idéal $\mathfrak{p} = \mathfrak{P}^{r_t}$ est situé dans le corps k_z et il est un idéal premier de ce corps du premier degré. Dans le corps de décomposition k_z, $p = \mathfrak{p}\mathfrak{a}$, où $\mathfrak{a}$ est un idéal premier avec $\mathfrak{p}$.

Démonstration. — La norme relative de l'idéal premier $\mathfrak{P}$ par rapport au corps k_z est $N_{k_z}(\mathfrak{P}) = \mathfrak{P}^{r_z}$. Pour trouver la plus petite puissance de l'idéal premier $\mathfrak{P}$ située dans k_z, supposons qu'on ait trouvé le plus grand commun diviseur des nombres entiers de k_z qui sont divisibles par $\mathfrak{P}$. Ce nombre est nécessairement un idéal premier $\mathfrak{p}$ de k_z, et comme $\mathfrak{P}^{r_z}$ est dans k_z, $\mathfrak{p}$ est certainement une puissance de $\mathfrak{P}$, soit $\mathfrak{p} = \mathfrak{P}^u$. Pour déterminer u, nous ferons les considérations suivantes. Soit A un nombre de K qui n'est pas divisible par $\mathfrak{P}$ et qui satisfait à $A \equiv zA$ suivant $\mathfrak{P}$ et si $A \equiv P^i$ suivant $\mathfrak{P}$, $i \equiv pi$ suivant $p^f - 1$, et, par suite, i est divisible par $1 + p + p^2 + \dots + p^{f-1}$, c'est-à-dire qu'il n'y a que $p - 1$ nombres incongrus suivant $\mathfrak{P}$ de la forme considérée; on a donc $A \equiv a$ suivant $\mathfrak{P}$, où a est un nombre entier rationnel. De là, il résulte en particulier que tout nombre α du corps k_z est congru à un nombre rationnel a suivant $\mathfrak{P}$, et par suite aussi suivant $\mathfrak{p}$, c'est-à-dire que $\mathfrak{p}$ est un idéal premier du premier degré du corps k_z et la norme de $\mathfrak{p}$ dans ce corps $k_z = p$.

D'autre part, dans le corps K, la norme de $\mathfrak{p}$ satisfait à $N(\mathfrak{p}) = n(\mathfrak{p})^{r_z}$, et à cause de $\mathfrak{p} = \mathfrak{P}^u$ et de $N(\mathfrak{P}) = p^f$, il résulte $p^{uf} = p^{r_z}$, c'est-à-dire $u = r_t$.

La définition du corps de décomposition donne $N(\mathfrak{P}) = \mathfrak{P}^{r_z}\mathfrak{A}$, où $\mathfrak{A}$ est un idéal premier avec $\mathfrak{P}$. Si $p = \mathfrak{p}\mathfrak{a}$, on a $N(\mathfrak{P}) = p^f = \mathfrak{p}^f\mathfrak{a}^f$, et, par suite, $\mathfrak{a}^f = \mathfrak{A}$, ce qui démontre la dernière partie du théorème 70.

§ 41. — Le corps de ramification d'un idéal premier $\mathfrak{P}$.

Nous allons étudier de plus près la nature du corps d'inertie et désigner par Λ un nombre bien déterminé du corps K divisible par $\mathfrak{P}$ et non par $\mathfrak{P}^2$, et nous déterminerons pour toutes les substitutions du corps d'inertie $t, t', t'', \ldots$ les congruences

$$\left.\begin{array}{l} t\Lambda \equiv P^{a}\Lambda \\ t'\Lambda \equiv P^{a'}\Lambda \\ t''\Lambda \equiv P^{a''}\Lambda \end{array}\right\} (\mathfrak{P}^2),$$

où $a, a', a'', \ldots$ sont des nombres de la suite $0, 1, 2, \ldots, p^f - 2$.

Parmi ces substitutions $t, t', t'', \ldots$, désignons par $v, v', v'', \ldots$ celles qui correspondent à la valeur zéro des exposants a, a', a'', soit r_v leur nombre; elles forment, il est facile de le voir, un sous-groupe invariant du groupe d'inertie. Nous désignerons ce sous-groupe de degré r_v par le nom de *sous-groupe de ramification* (Verzweigungsgruppe) *de l'idéal premier* $\mathfrak{P}$, et nous écrirons g_v. Le corps k_v qui lui appartient sera dit le *corps de ramification de l'idéal premier* $\mathfrak{P}$.

Le théorème suivant caractérise les rapports du groupe de ramification et du groupe d'inertie.

Théorème 71. — Le groupe de ramification g_v est un sous-groupe invariant du groupe d'inertie; son degré est une puissance de p, soit $r_v = p^l$. On obtient toutes les substitutions du groupe d'inertie et on n'obtient qu'une fois chacune d'elles, en multipliant chaque substitution du groupe de ramification par $1, t, t^2, \ldots, t^{h-1}$, où $h = \frac{r_t}{r_v}$ et où t est une substitution convenablement choisie du groupe d'inertie: h est un diviseur de $p^f - 1$.

Démonstration. — Soit $\mathfrak{P}^u$ une puissance assez élevée de $\mathfrak{P}$ pour que pour toute substitution v du groupe de ramification différente de 1, on ait $v\Lambda \not\equiv \Lambda$ suivant $\mathfrak{P}^u$. Posons $v\Lambda \equiv \Lambda + B\Lambda^2$ suivant $\mathfrak{P}^3$, B désignant un entier de K, il en résulte que $v^p\Lambda \equiv \Lambda$ suivant $\mathfrak{P}^3$, et, de même, $v^{p^2}\Lambda \equiv \Lambda$ suivant $\mathfrak{P}^4$ et ainsi de suite; enfin, $v^{p^{u-2}}\Lambda \equiv \Lambda$ suivant $\mathfrak{P}^u$. Il en résulte que $v^{p^{u-2}} = 1$, c'est-à-dire que le degré r_v du groupe de décomposition est une puissance de p; soit $r_v = p^l$.

Soit maintenant a le plus petit parmi les exposants $a, a', a'', \ldots$ qui ne sont pas nuls, et soit h le nombre de ces exposants distincts. Tous ces nombres seront des multiples de a et coïncident avec $0, a, 2a, \ldots, (h-1)a$; et, de plus, $ha = p^f - 1$. Nous reconnaissons en même temps que toutes les substitutions du groupe d'inertie peuvent être mises sous la forme $t^i v$, où i prend les valeurs $0, 1, \ldots, h-1$, et où v parcourt toutes les substitutions du groupe de ramification g_v. On a donc

$$r_t = h r_v.$$

§ 42. — Un théorème relatif au corps d'inertie.

Le théorème suivant va nous expliquer comment se comportent les idéaux $\mathfrak{P}$ et $\mathfrak{p}$ dans le corps k_t.

Théorème 72. — Tout nombre du corps K est congru suivant $\mathfrak{P}$ à un nombre du corps d'inertie. Le corps d'inertie ne décompose pas $\mathfrak{p}$, mais il en élève le degré, en ce que $\mathfrak{p}$, en passant du corps k_z, où il est un idéal premier du premier degré, se transforme en passant dans le corps supérieur k_t en un idéal premier du degré f.

Démonstration. — Posons

$$\pi = \{vP, v'P, v''P, \ldots\}^{p^{l(f-1)}},$$

$$\varkappa = \frac{1}{h}(\pi + t\pi + t^2\pi + \ldots + t^{h-1}\pi);$$

nous entendons par P un nombre primitif suivant $\mathfrak{P}$ et par t une substitution comme au théorème 71, le nombre π est un nombre du corps k_v et le nombre $\varkappa$ est situé dans le corps k_t. Pour le démontrer, il suffit de se rappeler que $\varkappa$ reste inaltéré lorsqu'on lui applique la substitution t, car t^h appartient à g_v et parce que les nombres π, $t\pi$, ..., $t^{h-1}\pi$ ne sont pas altérés par une substitution appartenant à g_v. Ces deux nombres π et $\varkappa$ sont tous deux congrus suivant l'idéal premier $\mathfrak{P}$ au nombre primitif P. Comme par suite k_t contient exactement p^f nombres incongrus suivant $\mathfrak{P}$, $\mathfrak{p} = \mathfrak{P}^{e}$ ne peut se décomposer dans le corps k_t et il est dans ce corps un idéal premier de degré f.

§ 43. — Théorèmes relatifs au groupe de ramification et au corps de ramification.

Il est facile dès lors d'établir la propriété caractéristique du groupe de ramification et qui est la suivante :

Théorème 73. — Le groupe de ramification g_v se compose de toutes les substitutions s qui, appliquées à tous les nombres entiers Ω du corps K, donnent la congruence

$$s\Omega \equiv \Omega \text{ suivant } \mathfrak{P}^2.$$

Démonstration. — Soit Ω de K congru à ω du corps d'inertie suivant $\mathfrak{P}$, posons par suite $\Omega - \omega \equiv B\Lambda$ suivant $\mathfrak{P}^2$, où Λ a le sens du paragraphe 41 et où B est un nombre convenablement choisi du corps K. Si nous appliquons une substitution r du corps de ramification, il vient $r\Omega - \omega \equiv r(B\Lambda) \equiv B\Lambda \equiv \Omega - \omega$, c'est-à-dire $r\Omega \equiv \Omega$ suivant $\mathfrak{P}^2$.

On reconnaît de plus facilement que l'on a :

THÉORÈME 74. — L'idéal $\mathfrak{p}_t = \mathfrak{P}^{r_t}$ est situé dans le corps de ramification, dans lequel il a le degré f, et l'on voit que, dans le corps de ramification, l'idéal $\mathfrak{p} = \mathfrak{p}_v^h$ se décompose en h facteurs premiers égaux.

§ 44. — LES CORPS DE RAMIFICATION SOULIGNÉS D'UN IDÉAL PREMIER $\mathfrak{P}$.

Nous nous proposons maintenant d'examiner de plus près la séparation de l'idéal $\mathfrak{p}_v$ en facteurs égaux.

Nous désignerons par L le plus grand exposant tel que pour toute substitution v du groupe de ramification, tous les nombres entiers du corps K satisfassent à $v\Omega \equiv \Omega$ suivant $\mathfrak{P}^L$, et nous déterminerons toutes les substitutions s du groupe de ramification, telles que $s\Omega \equiv \Omega$ suivant $\mathfrak{P}^{L+1}$; elles forment un sous-groupe $g_{\bar{v}}$ du groupe de ramification que nous appellerons *le groupe de ramification une fois souligné de l'idéal premier* $\mathfrak{P}$. Le corps $k_{\bar{v}}$ correspondant à $g_{\bar{v}}$ sera dit le *corps de ramification une fois souligné de l'idéal* $\mathfrak{P}$.

Voici les propriétés les plus importantes de ce corps.

THÉORÈME 75. — Le groupe de ramification une fois souligné $g_{\bar{v}}$ est un sous-groupe du groupe de ramification g_v. Soit $r_{\bar{v}} = p^{\bar{l}}$ son degré. On obtient toutes les substitutions de g_v et on ne les obtient qu'une fois, en multipliant toutes les substitutions du groupe de ramification souligné une fois $g_{\bar{v}}$ par certaines substitutions en nombre $p^{\bar{e}}$, $v_1, v_2, \ldots, v_{p^{\bar{e}}}$ du groupe de ramification : ici ces $p^{\bar{e}}$ substitutions offrent cette particularité que pour deux quelconques d'entre elles v_i, $v_{i'}$, on ait toujours une relation de la forme $v_i v_{i'} = v_{i'} v_i \bar{v}$, où $\bar{v}$ est une substitution de $g_{\bar{v}}$. L'idéal $\mathfrak{p}_{\bar{v}} = \mathfrak{P}^{r_{\bar{v}}}$ est un idéal premier dans $k_{\bar{v}}$; et, par suite, dans $k_{\bar{v}}$, l'idéal $\mathfrak{p}_v = \mathfrak{p}_{\bar{v}}^{p^{\bar{e}}}$ se sépare en $p^{\bar{e}}$ facteurs premiers égaux ; et $\bar{e}$ est un exposant qui ne dépasse pas le degré f de l'idéal premier $\mathfrak{P}$.

Démonstration. — Soit A un entier de K divisible par $\mathfrak{P}$ et non par $\mathfrak{P}^2$; déterminons un système de substitutions $v_1, \ldots, v_r$ du groupe de ramification tel que, si l'on pose

$$v_1 A \equiv A + B_1 A^L, \quad \ldots, \quad v_r A \equiv A + B_r A^L, \quad (\mathfrak{P}^{L+1})$$

les nombres entiers $B_1, \ldots, B_r$ soient tous incongrus suivant $\mathfrak{P}$, et tel qu'on ne puisse ajouter à ce système $v_1, \ldots, v_r$ de nouvelle substitution qui ne soit en contradiction avec la dernière condition.

Choisissons alors une substitution quelconque v^* du groupe de ramification g_r et posons $v^* A \equiv A + BA^L$ suivant $\mathfrak{P}^{L+1}$. B sera congru à l'un des nombres $B_1, \ldots, B_r$ suivant $\mathfrak{P}$; soit, par exemple, $B \equiv B_i$ suivant $\mathfrak{P}$, il en résulte que $v_i^{-1} v^* A \equiv A$ suivant $\mathfrak{P}^{L+1}$. Le théorème 72 nous apprend que tout nombre entier Ω de K est congru

à une expression $\alpha_l + \beta_l \Lambda + \ldots + \lambda_l \Lambda^l$ suivant $\mathfrak{P}^{L+1}$, où $\alpha_l, \beta_l, \ldots, \lambda_l$ sont des nombres entiers du corps d'inertie, et il s'ensuit que Ω satisfait à $v_l^{-1} v^* \Omega \equiv \Omega$ suivant $\mathfrak{P}^{L+1}$, c'est-à-dire que $v_l^{-1} v^* = \bar{v}$ ou que $v^* = v_l \bar{v}$. Cette égalité démontre les propriétés du groupe $g_{\bar{v}}$ affirmées au théorème 75.

Posons $r_l = p^l$ et soit $\bar{e} = l - \bar{l}$.

On voit comment il faut poursuivre la méthode. Soit $\bar{L}$ l'exposant le plus élevé, tel que pour toute substitution $\bar{v}$ tous les nombres du corps K satisfont à la congruence $\bar{v}\Omega \equiv \Omega$ suivant $\mathfrak{P}^{\bar{L}}$, nous déterminerons toutes les substitutions $\bar{\bar{v}}$ pour lesquelles on a constamment $\bar{\bar{v}}\Omega \equiv \Omega$ suivant $\mathfrak{P}^{\bar{L}+1}$. Ces substitutions forment un sous-groupe invariant $g_{\bar{\bar{v}}}$ du groupe $g_{\bar{v}}$, *le groupe de ramification deux fois souligné de l'idéal premier* $\mathfrak{P}$, soit $r_{\bar{\bar{l}}} = p^{\bar{\bar{l}}}$ son degré; posons $\bar{\bar{e}} = \bar{l} - \bar{\bar{l}}$, on a $\mathfrak{p}_{\bar{r}} = \mathfrak{p}_{\bar{\bar{r}}}^{p^{\bar{\bar{e}}}}$, où $\mathfrak{p}_{\bar{\bar{r}}}$ est un idéal premier du corps $k_{\bar{\bar{v}}}$ qui correspond à $g_{\bar{\bar{v}}}$.

En continuant ainsi nous atteindrons *le groupe de ramification trois fois souligné* et ainsi de suite. Supposons que *le groupe de ramification i fois souligné de l'idéal premier* $\mathfrak{P}$ soit celui qui ne contient plus que la substitution 1; *le corps de ramification i fois souligné de l'idéal premier* $\mathfrak{P}$ est alors le corps K lui-même et la nature de g_v nous est alors parfaitement connue. Il est évident qu'il ne peut exister de corps de ramification soulignés de l'idéal premier $\mathfrak{P}$, que si le degré M du corps K est divisible par p.

§ 45. — Un résumé rapide des théorèmes relatifs a la décomposition d'un nombre premier rationnel p dans le corps de Galois.

Les théorèmes démontrés du paragraphe 39 au paragraphe 44 nous montrent tout à fait ce qui se passe lorsqu'on décompose un nombre premier rationnel p dans un corps de Galois.

S'il s'agit d'un facteur déterminé $\mathfrak{P}$ de p, nous commencerons par mettre p sous la forme $p = \mathfrak{p}\mathfrak{a}$ dans le corps de décomposition de $\mathfrak{P}$, où $\mathfrak{p}$ est un idéal premier du premier degré et où $\mathfrak{a}$ est un idéal du corps de décomposition qui n'est pas divisible par $\mathfrak{p}$.

Le corps de décomposition de $\mathfrak{P}$ est contenu comme sous-corps dans le corps d'inertie de $\mathfrak{P}$, qui, de son côté, ne produit aucune décomposition de $\mathfrak{p}$, mais qui a fait de $\mathfrak{p}$ un idéal premier de degré f. Si le corps K est lui-même le corps de décomposition ou le corps d'inertie, ce premier pas termine la décomposition. Sinon $\mathfrak{p}$ peut encore être décomposé en d'autres facteurs dans K, ainsi $\mathfrak{p}$ devient d'abord dans le corps de ramification la puissance d'un idéal premier $\mathfrak{p}_r$, dont l'exposant est contenu dans $p^f - 1$ et n'est par suite pas divisible par p.

La condition nécessaire et suffisante pour que la décomposition de $\mathfrak{p}$ soit alors

terminée, est que p ne soit pas contenu dans le degré du groupe d'inertie et que, par suite, le corps K soit lui-même le corps de ramification.

Dans les corps de ramification soulignés, la décomposition se poursuit sans cesse et les exposants des puissances sont de la forme $p^{\bar{e}}$, $p^{\bar{\bar{e}}}$, ... et aucun des exposants $\bar{e}$, $\bar{\bar{e}}$ ne dépasse le degré f de l'idéal premier $\mathfrak{P}$.

La table qui va suivre donne une vue d'ensemble sur les résultats; la première ligne désigne les corps, la seconde les degrés des groupes correspondants, la troisième les degrés des corps, la quatrième leur degré relatif par rapport au corps immédiatement inférieur, la cinquième les idéaux premiers des corps et leurs représentations au moyen des puissances de $\mathfrak{P}$.

Nous admettrons que K est un corps de ramification trois fois souligné.

Tous les nombres indiquant les degrés ou les exposants dans cette table ont pour tout idéal premier du corps K qui divise p les mêmes valeurs que pour $\mathfrak{P}$; ils sont, par suite, parfaitement déterminés par p.

k_z	k_t	k_v	$k_{v'}$	$k_{v''}$	K
r_z	r_t	r_v	$r_{v'}$	$r_{v''}$	1
$m_z = \frac{M}{r_z}$	$m_t = \frac{M}{r_t}$	$m_v = \frac{M}{r_v}$	$m_{v'} = \frac{M}{r_{v'}}$	$m_{v''} = \frac{M}{r_{v''}}$	M
	$f = \frac{r_z}{r_t}$	$h = \frac{r_t}{r_v}$	$p^{e''} = \frac{r_v}{r_{v'}}$	$p^{e'} = \frac{r_{v'}}{r_{v''}}$	$p^{e} = r_{v''}$
$\mathfrak{p} = \mathfrak{p}_t^h = \mathfrak{P}^{r_t}$		$\mathfrak{p}_t = \mathfrak{p}_v^{p^{e''}} = \mathfrak{P}^{r_v}$	$\mathfrak{p}_v = \mathfrak{p}_{v'}^{p^{e'}} = \mathfrak{P}^{r_{v'}}$	$\mathfrak{p}_{v'} = \mathfrak{P}^{p^{e}} = \mathfrak{P}^{r_{v''}}$	$\mathfrak{P}$

CHAPITRE XI.

Les differentes et les discriminants du corps de Galois et de ses sous-corps.

§ 46. Les différentes du corps d'inertie et des corps de ramification.

En rapprochant les résultats que nous venons d'acquérir de ceux du chapitre V, nous aurons une source de vérités nouvelles. C'est ainsi, qu'en vertu du paragraphe 41, nous pouvons énoncer un théorème qui va nous donner les propriétés les plus importantes du corps d'inertie.

Théorème 76. — La différente du corps d'inertie relatif à l'idéal premier $\mathfrak{P}$ n'est pas divisible par $\mathfrak{P}$. Le corps d'inertie comprend tous les sous-corps de K dont les différentes ne sont pas divisibles par $\mathfrak{P}$.

En ce qui concerne les différentes des corps de ramification, on a les théorèmes suivants :

Théorème 77. — La différente relative du corps de ramification par rapport au corps d'inertie est divisible par $\mathfrak{P}^{r_t - r_v} = \mathfrak{p}_v^{h-1}$, et elle n'est pas divisible par une puissance supérieure de $\mathfrak{P}$.

Démonstration. — Soit α un nombre entier de k_v qui est divisible par $\mathfrak{p}_v = \mathfrak{P}^{r_v}$, mais qui ne l'est pas par $\mathfrak{p}^2$, et soit A un nombre de K divisible par $\mathfrak{P}$, mais ne contenant pas $\mathfrak{P}^2$.

Posons $\frac{\alpha}{A^{r_v}} \equiv P^c$ suivant $\mathfrak{P}$, P désignant un nombre primitif suivant $\mathfrak{P}$, on a $\alpha \equiv P^c A^{r_v}$ suivant $\mathfrak{p}_v \mathfrak{P}$. Soit dès lors t^* une substitution quelconque du corps d'inertie qui n'appartient pas à g_v et supposons que $t^* A \equiv P^{a^*} A$ suivant $\mathfrak{P}^2$, où a^* est l'un des nombres $a, 2a, \ldots, (h-1)a$ [voir § 41], il en résultera que

$$t^* \alpha \equiv P^{c + a^* r_v} A^{r_v} \equiv P^{a^* r_v} \alpha, \ (\mathfrak{p}_v \mathfrak{P}).$$

Comme r_v est une puissance de p, $P^{a^* r_v} \not\equiv 1$ suivant $\mathfrak{P}$, et, par suite, $\alpha - t^* \alpha$ ne peut être divisible par $\mathfrak{p}_v \mathfrak{P}$, il est donc exactement divisible par $\mathfrak{p}_v = \mathfrak{P}^{r_v}$. Si, de plus, ω est un nombre quelconque de k_v, ce nombre, d'après le théorème 72, est nécessairement congru suivant $\mathfrak{P}$ à un nombre ω_t du corps d'inertie; il en résulte que $\omega - t^* \omega \equiv 0$ suivant $\mathfrak{p}_v$. D'où nous pouvons conclure que la différente considérée est exactement divisible par $\mathfrak{P}^{(h-1) r_v} = \mathfrak{P}^{r_t - r_v}$.

On démontre de même le fait suivant :

THÉORÈME 78. — La différente relative du corps de ramification souligné une fois par rapport au corps de ramification k_v, contient exactement $\mathfrak{P}^{L(r_v - r_{\bar{v}})} = \mathfrak{p}_{\bar{v}}^{L(p^{e'}-1)}$. La différente relative du corps de ramification deux fois souligné $k_{\bar{\bar{v}}}$ par rapport à $k_{\bar{v}}$ contient exactement $\mathfrak{P}^{L'(r_{\bar{v}} - r_{\bar{\bar{v}}})} = \mathfrak{p}_{\bar{\bar{v}}}^{L'(p^{e''}-1)}$ et ainsi de suite.

§ 47. — LES DIVISEURS DES DISCRIMINANTS DU CORPS DE GALOIS.

THÉORÈME 79. — Le nombre premier rationnel p est contenu dans le discriminant D du corps K à une puissance dont l'exposant est :

$$m_t\{r_t - r_v + L(r_v - r_{\bar{v}}) + L'(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \ldots\}.$$

Démonstration. — Le théorème 41 rapproché des théorèmes 76, 77, 78 nous apprend que la différente D du corps K contient l'idéal premier $\mathfrak{P}$ exactement à la puissance

$$r_t - r_v + L(r_v - r_{\bar{v}}) + L'(r_{\bar{v}} - r_{\bar{\bar{v}}}) + \ldots$$

le théorème 68 exige alors l'exactitude de notre proposition.

Dans le cas où il n'existe pas de corps ramifié souligné, l'exposant de p prend dans D la valeur $m_t(r_t - 1)$.

D'après ce qui précède, ce cas se présentera toutes les fois que p est premier avec M.

Ce résultat est à comparer aux remarques du paragraphe 12.

THÉORÈME 80. — L'exposant de la puissance du nombre premier rationnel p contenue dans le discriminant D ne dépasse pas une certaine limite qui ne dépend que du degré M du corps de Galois K.

Démonstration. — Tous les exposants L, L', ... qui correspondent à un certain idéal premier $\mathfrak{P}$ sont inférieurs à une limite déterminée par le nombre M. Pour trouver la limite de L, nous désignerons par ω un nombre entier de $k_{\bar{v}}$ divisible par $\mathfrak{p}_{\bar{v}}$, mais non divisible par $\mathfrak{p}_{\bar{v}}^2$, et nous choisirons un système de p^e substitutions $v_1, v_2, \ldots, v_{p^e}$ du groupe de ramification, tels qu'en les composant avec $g_{\bar{v}}$ on obtienne g_v. Le nombre

$$\alpha = v_1\omega + v_2\omega + \ldots + v_{p^e}\omega$$

ne sera pas altéré par une substitution de g_v ; il appartient au corps k_v. D'autre part, $\omega \equiv v\omega$ suivant $\mathfrak{P}^L$, et, par suite, $\alpha \equiv p^e\omega$ suivant $\mathfrak{P}^L$.

Si donc on avait $L > er_t + r_v$, on aurait $\alpha \equiv 0$ suivant $\mathfrak{p}^e\mathfrak{p}_v$ et $\equiv 0$ suivant $\mathfrak{p}^e\mathfrak{p}_v\mathfrak{P}$. Si donc l'on fait $p = \mathfrak{p}\mathfrak{a}$, où $\mathfrak{a}$ est un idéal du corps de décomposition premier avec $\mathfrak{p}$, et si l'on désigne par γ un nombre de ce corps divisible par $\mathfrak{a}$ et premier avec $\mathfrak{p}$, $\beta = \frac{\alpha\gamma^e}{p^e}$ est un nombre entier de k_v ; ce nombre serait divisible par $\mathfrak{p}_v$ et ne

le serait pas par $\mathfrak{p}, \mathfrak{P}$, et, par suite, contrairement au théorème 75, $\mathfrak{p}_r$ serait un idéal du corps k_r. Comme on peut trouver de même une limite supérieure pour les autres exposants L, ..., on voit que l'exposant (indiqué au théorème 79) de la puissance de p contenue dans D ne peut dépasser une certaine limite qui ne dépend que du degré M du corps K.

Le théorème 80 a d'autant plus d'importance qu'il limite *a priori* le nombre des nombres premiers contenus dans M. Rangeons dans un même type tous les corps de degré M pour lesquels la décomposition en facteurs premiers de M donne les mêmes valeurs pour les nombres considérés précédemment. Nous pouvons affirmer que, pour une valeur donnée de M, il n'y a qu'un nombre limité de types de corps possibles.

Comme exemple du théorème 80, nous indiquerons le corps quadratique (traité complètement dans la troisième partie de ce livre) et dont le discriminant contient tout nombre premier impair au plus à la première puissance et le nombre premier 2 au plus à la troisième. (Voir § 59, théorème 95.)

CHAPITRE XII.

Les rapports entre les propriétés arithmétiques et les propriétés algébriques du corps de Galois.

§ 48. Le corps de Galois relatif, le corps abélien relatif, le corps cyclique relatif.

Lorsque le groupe G des substitutions $s_1, \ldots, s_M$ d'un groupe de Galois forme un groupe abélien, c'est-à-dire lorsque les substitutions $s_1, \ldots, s_M$ peuvent se permuter entre elles, le corps de Galois K est un corps *abélien*.

En particulier, si ce groupe de substitutions G est cyclique, c'est-à-dire si les M substitutions $s_1, \ldots, s_M$ peuvent toutes être représentées par des puissances de l'une d'entre elles, le corps abélien K est dit un *corps cyclique*.

En appliquant aux substitutions d'un groupe abélien les considérations faites au numéro 28 pour les classes d'ideaux, on arrive au théorème : tout corps abélien est composé de corps cycliques. D'autre part, les corps cycliques se composent à leur tour de corps cycliques particuliers, ceux dont le degré est un nombre premier ou la puissance d'un nombre premier.

Ces notions peuvent être généralisées ainsi :

Soit Θ une racine de l'équation de degré l :

$$\Theta^l + \alpha_1 \Theta^{l-1} + \ldots + \alpha_l = 0,$$

dont les coefficients $\alpha, \ldots, \alpha_l$ appartiennent à un corps k de degré m. Supposons de plus cette équation irréductible dans le domaine k de rationalité et qu'elle ait la propriété suivante, les $l-1$ autres racines $\Theta', \ldots, \Theta^{l-1}$ de cette équation sont des fonctions entières rationnelles de Θ dont les coefficients sont des nombres de k.

Le corps de nombre K composé de Θ et des nombres de k est dit alors un *corps de Galois relatif par rapport au corps k* de degré $M = lm$.

Le degré l de l'équation précédente est le degré relatif de K.

Si l'on pose $\Theta = S_1\Theta$, $\Theta' = S_2\Theta$, $\Theta^{l-1} = S_l\Theta$, le groupe des substitutions S_1, S_2, ..., S_l est appelé le *groupe relatif*; si ce groupe est abélien, le corps K *est dit un corps abélien relatif par rapport à k*. Si ce groupe relatif est cyclique, le corps K est dit *cyclique relatif* par rapport à k.

§ 49. — Les propriétés algébriques du corps d'inertie et du corps de ramification. — La représentation des nombres du corps de Galois par des radicaux dans le domaine du corps de décomposition.

A l'aide des notions que nous venons de définir, nous pourrons énoncer très simplement quelques propriétés algébriques importantes du corps de décomposition et du corps d'inertie, ainsi que des corps de ramification, qui sont d'ailleurs une conséquence des propriétés de leurs groupes démontrées plus haut.

Théorème 81. — Le corps d'inertie k_t est un corps cyclique relatif de degré relatif f par rapport au corps de décomposition k_z. Le corps de ramification k_v est cyclique relatif de degré relatif h par rapport à k_t. Le corps de ramification une fois souligné $k_{\underline{v}}$ est un corps abélien relatif de degré relatif p^e par rapport à k_v; le corps $k_{\underline{\underline{v}}}$ est un corps abélien relatif de degré relatif p^e par rapport à $k_{\underline{v}}$ et ainsi de suite. Les groupes abéliens relatifs des corps $k_{\underline{v}}$, $k_{\underline{\underline{v}}}$ ... ne contiennent que des substitutions de degré p.

D'après ce théorème 81, la séparation en facteurs égaux s'opère au moyen d'une suite d'équations abéliennes, et ce résultat exprime une propriété surprenante et nouvelle du corps de décomposition.

Théorème 82. — Le corps de décomposition de tout idéal premier dans K détermine un domaine de rationalité, dans lequel les nombres du corps primitif K s'expriment uniquement au moyen de radicaux.

Ce théorème 82 met bien en lumière toute l'importance des équations solubles par radicaux; car il montre que dans le problème de la décomposition des nombres en idéaux premiers, les solutions les plus importantes et les plus difficiles se présentent pour les corps relatifs, dont les nombres peuvent être représentés au moyen de radicaux dans certains domaines de rationalité.

§ 50. La densité des idéaux premiers du premier degré et le rapport entre cette densité et les propriétés algébriques du corps.

C'est un fait merveilleux que la fréquence de certains idéaux premiers du premier degré d'un corps permet de conclure des propositions relatives à la nature algébrique de ce corps. [Kronecker [14].]

Soit k un corps quelconque de degré m et soit p_i un nombre premier rationnel qui peut se décomposer exactement en i idéaux premiers distincts du premier degré. Si la limite

$$\mathop{L}_{s=1}\left(\frac{\sum\limits_{(p_i)}\frac{1}{p_i^s}}{\log\left(\frac{1}{s-1}\right)}\right)$$

existe, en supposant que la somme écrite au numérateur s'étende à tous les nombres premiers p_i, nous dirons que les nombres premiers de l'espèce p_i ont une densité; si cette limite a pour valeur Δ_i, nous dirons que Δ_i est la *densité* des nombres premiers de la forme p_i. Kronecker admet implicitement, dans ses recherches, que les nombres premiers des m sortes $p_1, p_2, \ldots, p_m$ ont une densité. La vérité de cette hypothèse n'a pas encore été démontrée (¹). Par contre, on arrive à démontrer le théorème suivant :

Théorème 83. — Si $m-1$ sortes de nombres premiers parmi les m sortes $p_1, \ldots, p_m$ d'un corps de degré m ont une densité, la m^e aussi a une densité et on a entre les m densités la relation

$$\Delta_1 + 2\Delta_2 + \ldots + m\Delta_m = 1.$$

Démonstration. — Employant la deuxième expression de $\zeta(s)$ indiquée au numéro 27 et prenant le logarithme, il vient

$$\log\zeta(s) = \sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^s} + S,$$

$$S = \frac{1}{2}\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3}\sum_{(\mathfrak{p})}\frac{1}{n(\mathfrak{p})^{3s}} + \ldots,$$

(¹) Dans le cas où le groupe de l'équation qui détermine k est le groupe symétrique, les remarques de [Kronecker permettent de déterminer les densités $\Delta_1, \ldots, \Delta_m$; Frobenius a démontré l'existence de ces densités et a déterminé leurs valeurs; ce sont des nombres rationnels qui dépendent du groupe de l'équation de k. [Frobenius [1].]

où les sommes s'étendent à tous les idéaux premiers $\mathfrak{p}$ du corps. Désignons par $\mathfrak{p}_1$ les idéaux premiers du premier degré; nous aurons évidemment

$$(19)\qquad \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} = \sum_{(p_1)} \frac{1}{p_1^s} + \sum_{(p_2)} \frac{2}{p_2^s} + \ldots + \sum_{(p_m)} \frac{m}{p_m^s}$$

où la somme du premier membre s'étend à tous les idéaux du premier degré et où la somme du second membre s'étend à tous les nombres premiers rationnels $p_1, p_2, \ldots, p_m$.

Nous remarquons, d'autre part, que pour tous les idéaux $\mathfrak{p}$ de degré supérieur au premier $n(\mathfrak{p}) \geqq p^2$, et qu'un nombre premier quelconque p contient au plus m idéaux premiers; il en résulte que

$$\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} - \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} < m \sum_{(p)} \frac{1}{p^{2s}} < m \sum_{(h)} \frac{1}{h^2},$$

où la dernière somme s'étend à tous les entiers $h > 1$.

On trouve de même que

$$S < m \left\{ \sum_{(h)} \frac{1}{h^2} + \sum_{(h)} \frac{1}{h^3} + \ldots \right\} = m \sum_{(h)} \frac{1}{h(h-1)} = m.$$

On déduit de ces inégalités que

$$\log \zeta(s) - \sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}$$

tend vers une limite finie pour $s = 1$.

D'après le théorème 56, $\log \zeta(s) - \log \frac{1}{s-1}$ tend aussi vers une limite finie pour $s = 1$; on peut en dire autant de

$$\sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s} - \log \frac{1}{s-1},$$

c'est-à-dire que

$$\underset{(s=1)}{\mathrm{L}} \frac{\sum_{(\mathfrak{p}_1)} \frac{1}{n(\mathfrak{p}_1)^s}}{\log \frac{1}{s-1}} = 1,$$

d'où, en tenant compte de (19), la vérité de notre affirmation.

Pour un corps de Galois K de degré M, on a $\Delta_1 = 0$, $\Delta_2 = 0$, ..., $\Delta_{m-1} = 0$, et, par suite, en vertu du théorème 83, le

Théorème 84. — Dans un corps de Galois de degré M, les nombres premiers p_M qui se décomposent en idéaux premiers du premier degré ont une densité, cette densité est $\Delta_M = \frac{1}{M}$.

Soit k un corps quelconque et K le corps de Galois de degré M formé de k et de ses conjugués k', ..., $k^{(m-1)}$, on reconnaît facilement que les nombres premiers p_m de k coïncident avec les nombres premiers p_M de k, et par suite les nombres premiers p_m de k ont une densité, et cette densité est égale à $\frac{1}{M}$, c'est-à-dire à l'inverse du degré de la résolvante de Galois. [Kronecker[14].]

CHAPITRE XIII.

La composition des corps de nombres.

§ 51. — Le corps de Galois composé d'un corps k et de ses conjugués.

Théorème 85. — Si des deux corps k_1 et k_2 on compose un corps K, le discriminant du corps composé contient comme facteurs premiers rationnels ceux contenus dans le discriminant de k_1, ou dans celui de k_2, ou dans les deux, et ne contient que ceux-là.

La démonstration de ce théorème résulte immédiatement du théorème 39. Une conséquence immédiate du théorème 85 est la suivante :

Théorème 86. — Si d'un corps k de degré m et de tous ses corps conjugués k', ..., $k^{(m-1)}$ on compose un corps de Galois K, le discriminant du corps K contient tous les facteurs premiers de k et il n'en contient pas d'autres.

§ 52. — La composition de deux corps dont les discriminants sont premiers entre eux.

Le cas de deux corps dont les discriminants sont premiers entre eux présente un intérêt particulier. Le théorème le plus important et le plus fertile de ce cas est le suivant :

Théorème 87. — Deux corps k_1 et k_2 de degrés respectifs m_1, m_2, dont les discriminants sont premiers entre eux, se composent toujours en un corps de degré $m_1 m_2$.

Démonstration. — Soit K_1 le corps de Galois composé de k_1 et de tous ses conjugués; le discriminant de K_1, d'après le théorème 86, est premier avec celui de k_2.

Soit z un nombre qui détermine k_1 ; ce nombre est racine d'une équation irréductible de degré m_1 à coefficients entiers et rationnels.

Si donc le corps composé de k_1 et de k_2 était d'un degré inférieur à $m_1 m_2$, cette équation se réduirait dans le domaine k_2, c'est-à-dire que z serait racine d'une équation de la forme

$$z^r + \alpha_1 z^{r-1} + \ldots + \alpha_r = 0$$

de degré $r < m_1$ et dont les coefficients $\alpha_1, \ldots, \alpha_r$ seraient des nombres de k_2. Soit k le corps de nombres formé avec $\alpha_1, \ldots, \alpha_r$. Comme $\alpha_1, \ldots, \alpha_r$ peuvent être exprimées rationnellement en fonction des racines de la dernière équation, k est un sous-corps de k_1, et comme k est aussi un sous-corps de k_2, le discriminant de k d'après le théorème 39 diviserait celui de k_1 et celui de k_2, et le discriminant de ce corps k serait égal à 1, ce qui est contraire au théorème 44.

Nous signalerons encore les faits suivants, faciles à vérifier.

Théorème 88. — *Si k_1 et k_2 sont deux corps, le premier de degré m_1, le second de degré m_2 de discriminants d_1 et d_2 premiers entre eux, le discriminant du corps composé K est $d_1^{m_2} d_2^{m_1}$.*

On obtient les nombres d'une base du corps K, en multipliant chacun des m_1 nombres d'une base du corps k_1, par chacun des m_2 nombres d'une base du corps k_2. Soit p un nombre rationnel qui se décompose en $p = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \ldots \mathfrak{p}_r^{e_r}$ dans k_1 et en $p = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_s$, où $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ sont des idéaux premiers distincts de k_1, et $\mathfrak{q}_1, \ldots \mathfrak{q}_s$ des idéaux distincts de k_2 ; on a dans K la décomposition $p = \prod_{i,l} \mathfrak{J}_{il}^{e_i}$, où le produit s'étend à $i = 1, \ldots, r$, $l = 1, \ldots, s$, et où $\mathfrak{J}_{il}$ est l'idéal de K défini comme étant le plus grand commun diviseur de $\mathfrak{p}_i$ et de $\mathfrak{q}_l$. Les idéaux $\mathfrak{J}_{il}$ ne sont pas nécessairement des idéaux premiers de K.

Lorsqu'on part de deux corps k_1, k_2 de discriminants quelconques, la solution de la question ne devient simple que si l'on fait des hypothèses restrictives sur la nature du corps et des nombres premiers que l'on veut décomposer. [Hensel [1].]

Les résultats exposés dans les chapitres X à XIII me semblent être les principes les plus importants d'une théorie des idéaux et des discriminants d'un corps de Galois. Les méthodes suivies pourraient encore être développées dans bien des directions, en particulier on pourrait étendre sans y changer beaucoup au corps de Galois relatif une série de théorèmes démontrés depuis le paragraphe 39 jusqu'au paragraphe 44. [Dedekind [2].]

CHAPITRE XIV.

Les idéaux premiers du premier degré et la notion de classe.

§ 53. — Les idéaux premiers du premier degré engendrent des classes d'idéaux.

Il est intéressant de voir que les principes développés dans les chapitres X-XII éclairent aussi la génération et la nature des classes d'idéaux. Nous exposerons dans ce chapitre et dans le suivant les théorèmes généraux importants relatifs à ces questions. Le premier théorème concerne la génération des classes d'idéaux d'un corps de Galois au moyen d'idéaux premiers du premier degré et s'énonce :

Théorème 89. — Dans toute classe d'idéaux d'un corps de Galois il y a des idéaux dont tous les facteurs premiers sont des idéaux du premier degré.

Nous démontrerons d'abord le

Lemme 12. — Soit K un corps de Galois de degré M et de discriminant D et $\mathfrak{P}$ un idéal premier de ce corps de degré $f > 1$ qui n'est pas contenu dans DM! ; il y a toujours dans K un nombre entier Ω premier avec DM!, divisible par $\mathfrak{P}$ et non par $\mathfrak{P}^2$, et dont tous les autres facteurs premiers sont de degré inférieur à f.

Démonstration. — Soit P un entier du corps K, tel que tout autre entier Ω soit congru à une fonction entière à coefficients entiers de P suivant $(\mathfrak{P})^2$. D'après le théorème 29, ce nombre existe. Désignons par $(\mathfrak{P}')$, ..., $(\mathfrak{P}^{(m)})$ les idéaux conjugués de $\mathfrak{P}$ et distincts de $\mathfrak{P}$, et déterminons un nombre A de K qui satisfait aux congruences

$$\mathsf{A} \equiv \mathsf{P} \quad (\mathfrak{P}^2),$$
$$\mathsf{A} \equiv 0 \quad (\mathfrak{P}'\mathfrak{P}''\ldots\mathfrak{P}^{(m)}),$$
$$\mathsf{A} \equiv 1 \quad (M!).$$

Et soit z une substitution du groupe de décomposition telle que $z\mathsf{P} \equiv \mathsf{P}^p$ suivant $\mathfrak{P}$, il est évident que les $f-1$ différences $\mathsf{A} - z\mathsf{A}$, $\mathsf{A} - z^2\mathsf{A}$, $\mathsf{A} - z^{f-1}\mathsf{A}$ sont premières avec $\mathfrak{P}$. Si, d'autre part, s est une substitution n'appartenant pas au groupe de décomposition, $s\mathsf{A}$ est divisible par $\mathfrak{P}$, et, par suite, la différence $\mathsf{A} - s\mathsf{A}$ est première avec $\mathfrak{P}$. La différente de A sera donc aussi première avec $\mathfrak{P}$, et il en résulte que A est un nombre qui détermine K, d'après une remarque antérieure. En tenant compte du théorème 31, on voit que K est le corps d'inertie de $\mathfrak{P}$ et, par conséquent, A satisfait à une équation de la forme

$$\mathsf{A}^f + \alpha_1\mathsf{A}^{f-1} + \ldots + \alpha_f = 0,$$

où $\alpha_1, \ldots, \alpha_f$ sont des nombres du corps de décomposition k de l'idéal premier $\mathfrak{P}$.

Nous désignerons par k', k'', ... les autres sous-corps de même degré $\frac{\mathrm{M}}{f}$; A est alors racine des équations

$$\mathsf{A}^f + \alpha_1' \mathsf{A}^{f-1} + \ldots + \alpha_f' = 0,$$
$$\mathsf{A}^f + \alpha_1'' \mathsf{A}^{f-1} + \ldots + \alpha_f'' = 0,$$
$$\ldots\ldots\ldots\ldots$$

α_1', ..., α_f' étant des nombres de k', α_1''; ..., α_f'' des nombres de k'', etc. Déterminons, dès lors, f nombres entiers rationnels tels que

$$a_1 \equiv \alpha_1, \ \ldots, \ a_f \equiv \alpha_f, \quad (\mathfrak{P});$$

ceci est possible, car, d'après le théorème 70, $\mathfrak{P}$ est du premier degré dans k. Soient ensuite b_1, ..., b_f, f entiers rationnels satisfaisant aux congruences

$$\mathrm{M}!\,b_1 \equiv a_1, \ \ldots, \ \mathrm{M}!\,b_f \equiv a_f, \quad (p),$$

et pour lesquels, de plus, aucune des différences appartenant à l'indice 1

$$\beta_1 = \mathrm{M}!\,b_1 - \alpha_1, \quad \beta_1' = \mathrm{M}!\,b_1 - \alpha_1', \ \ldots$$

ne s'annule.

Nous poserons, de plus,

$$\mathsf{B} = \mathsf{A}^f + \mathrm{M}!\,(b_1 \mathsf{A}^{f-1} + b_2 \mathsf{A}^{f-2} + \ldots + b_f).$$

Enfin, nous désignerons par q_1, ..., q_l les nombres premiers rationnels tous différents de p, qui sont contenus dans le discriminant A de A ou dans les normes des nombres β_1, β_1', ... et qui sont plus grands que M. Soit q_i un quelconque de ces nombres, il ne peut contenir dans K que M facteurs premiers au plus; il faudra donc que l'un des q_i nombres ($q_i > \mathrm{M}$), B, $\mathsf{B}+1$, $\mathsf{B}+2$, ..., $\mathsf{B}+q_i-1$, soit premier avec q_i; soit, par exemple, $\mathsf{B}+c_i$ un nombre premier avec q_i. Si l'on calcule un nombre entier rationnel c qui satisfait aux l congruences $\mathrm{M}!pc \equiv c_i$ suivant q_i pour $i = 1, 2, \ldots, l$,

$$\Omega = \mathsf{B} + \mathrm{M}!pc$$

est un nombre qui a les propriétés exigées par le lemme 12.

En effet : d'après la congruence $\mathsf{A} \equiv 1$ suivant M!, le nombre Ω est premier avec tous les nombres premiers rationnels $\leqq \mathrm{M}$; et, à cause des conditions qui nous ont servies à déterminer c, Ω est premier avec tous les nombres premiers rationnels contenus dans A et supérieurs à M. Le nombre Ω est donc premier avec tous les nombres premiers rationnels contenus dans A et différents de p.

De plus, Ω est divisible par $\mathfrak{P}$ et non par $\mathfrak{P}'$, $\mathfrak{P}''$, ..., $\mathfrak{P}^{(m)}$, car $\mathrm{M}!b_f - a_f \equiv 0$ suivant p. Le nombre Ω est de la forme

$$\Omega = \mathsf{A}^f + m_1 \mathsf{A}^{f-1} + \ldots + m_f.$$

où $m_1, \dots, m_f$ sont des entiers rationnels. Comme $\mathsf{A} \equiv \mathsf{P}$ suivent $\mathfrak{P}^2$ et que P ne peut satisfaire à aucune congruence de degré inférieur à $2f$ suivant $\mathfrak{P}^2$, Ω ne peut pas être divisible par $\mathfrak{P}^2$. Si, d'autre part, Ω était divisible par un idéal premier $\mathfrak{L}$ de degré $f' > f$ et si l'on désignait par $1, z', z'^2, \dots, z'^{f'-1}$ les f' substitutions du groupe de décomposition de $\mathfrak{L}$ par lesquelles ce dernier groupe résulte du groupe d'inertie, on aurait les f' congruences

$$\begin{aligned} &\mathsf{A}^f + m_1 \mathsf{A}^{f-1} + \dots + m_f \equiv 0, \quad (\mathfrak{L}), \\ &(z'\mathsf{A})^f + m_1 (z'\mathsf{A})^{f-1} + \dots + m_f \equiv 0, \quad (\mathfrak{L}), \\ &\dots\dots\dots\dots\dots\dots \end{aligned}$$

et ceci exigerait que le discriminant A de A soit divisible par $\mathfrak{L}$, ce qui n'a pas lieu.

Enfin, supposons que Ω soit divisible par un idéal premier $\mathfrak{L}$ de degré f; l'un des corps $k, k', k'', \dots$ serait le corps de décomposition de $\mathfrak{L}$, soit, par exemple, le corps k'.

Ecrivons alors Ω sous la forme

$$\Omega = (\mathsf{A}^f + \alpha_1' \mathsf{A}^{f-1} + \dots + \alpha_f') - \beta_1' \mathsf{A}^{f-1} + \dots + \beta_f',$$

où $\beta_1', \dots, \beta_f'$ sont des nombres de k'. Si $1, z', z'^2, \dots, z'^{f-1}$ sont les f substitutions qui font résulter le corps de décomposition de $\mathfrak{L}$ de son corps d'inertie, on voit que

$$\begin{aligned} &\beta_1' \mathsf{A}^{f-1} + \dots + \beta_f' \equiv 0, \quad (\mathfrak{L}), \\ &\beta_1' (z'\mathsf{A})^{f-1} + \dots + \beta_f' \equiv 0, \quad (\mathfrak{L}), \\ &\dots\dots\dots\dots\dots \end{aligned}$$

et ces congruences démontreraient que soit A, soit β_1', fut divisible par $\mathfrak{L}$, ce qui est contraire à ce qui précède.

Dans chaque classe on peut trouver un idéal premier avec DM!; on voit alors facilement, en tenant compte du lemme 12, qu'on a le droit d'affirmer le théorème 89. Kummer l'avait déjà démontré pour le corps circulaire (Kreiskörper). [Kummer[5].]

CHAPITRE XV.

Le corps relatif cyclique de degré premier.

54. — La puissance symbolique. — Un théorème sur les nombres de norme relative égale a 1.

Nous allons démontrer une série de théorèmes fondamentaux concernant les corps abéliens relatifs. Pour mieux pouvoir les énoncer et les démontrer, nous allons fixer quelques notations et quelques définitions.

Soit K un corps de nombres de degré lm, cyclique relatif par rapport au corps k

de degré m, le degré relatif l étant un nombre premier. Soient 1, S, S^2, ..., S^{l-1} les substitutions du groupe cyclique relatif. Enfin, nous définissons ainsi la notion de *puissance symbolique* d'un nombre A du corps K : Soit A un nombre quelconque de K entier ou fractionnaire et soient a, a_1, a_2, ..., a_{l-1} des nombres entiers rationnels quelconques, nous écrirons

$$\mathsf{A}^{a}(S\mathsf{A})^{a_1}(S\mathsf{A}^2)^{a_2}\dots(S^{l-1}\mathsf{A})^{a_{l-1}}$$

sous la forme abrégée

$$\mathsf{A}^{a+a_1S+a_2S^2+\dots+a_{l-1}S^{l-1}} = \mathsf{A}^{F(S)},$$

où F(S) désigne la fonction entière à coefficients entiers qui constitue l'exposant du premier membre. La puissance symbolique de degré F(S) de A est à son tour un nombre entier ou fractionnaire de K. Ces exposants symboliques peuvent être considérés comme une généralisation d'une notation introduite par Kronecker au sujet du corps circulaire. [Kronecker[1].]

Ceci posé, nous aurons une suite de théorèmes.

Théorème 90. — Tout nombre entier ou fractionnaire A de K dont la norme relative, par rapport à k, est égale à 1 peut être considéré comme la puissance symbolique de degré $(1-S)$ d'un certain nombre B du corps K.

Démonstration. — Soit x une variable et Θ un nombre qui détermine K ; posons

$$\mathsf{A}_x = \frac{x+\Theta}{x+S(\Theta)}\mathsf{A} = (x+\Theta)^{1-S}\mathsf{A}$$

et

$$\mathsf{B}_x = 1 + \mathsf{A}_x^{1} + \mathsf{A}_x^{1+S} + \mathsf{A}_x^{1+S+S^2} + \dots + \mathsf{A}_x^{1+S+S^2+\dots+S^{l-2}}$$

et remarquons qu'en vertu de l'hypothèse

$$\mathsf{A}^{1+S+\dots+S^{l-1}} = 1$$

et que, par suite, on a aussi

$$\mathsf{A}_x^{1+S+\dots+S^{l-1}} = 1,$$

il en résulte que

$$\mathsf{B}_x^{1-S} = \mathsf{A}_x ;$$

B_x est une fonction rationnelle de x qui n'est pas identiquement nulle ; on peut donc trouver un nombre $x = a$ tel que B_a ne soit pas nul dans K. Le nombre

$$\mathsf{B}^* = \frac{\mathsf{B}_a}{a+\Theta}$$

satisfait alors à

$$\mathsf{A} = \mathsf{B}^{*1-S}.$$

Posons $\mathsf{B}^* = \frac{\mathsf{B}}{b}$, où B désigne un entier algébrique de K et b un entier rationnel : on a aussi

$$\mathsf{A} = \mathsf{B}^{1-S}.$$

§ 55. — Le système des unités fondamentales relatives. — On démontre qu'elles existent.

Un deuxième théorème important concerne les unités du corps K. Supposons que, parmi les m corps conjugués déterminés par k, r_1 soient réels et qu'il y ait r_2 couples de corps imaginaires conjugués, d'après le théorème 47 le nombre des unités fondamentales de k est $r = r_1 + r_2 - 1$. Nous entendrons par *système d'unités fondamentales relatives* du corps K par rapport à k un système de $r + 1$ unités H_1, $\mathsf{H}_2, \dots, \mathsf{H}_{r+1}$ du corps K, telles qu'une unité de la forme

$$\mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{r+1}^{F_{r+1}(S)}[\varepsilon]$$

ne peut être la puissance symbolique de degré $(1 - S)$ d'une unité de K que si les entiers algébriques $F_1(\zeta), \dots, F_{(r+1)}(\zeta)$ sont tous divisibles par $1 - \zeta$.

Ici, $F_1(S), \dots, F_{(r-1)}(S)$ sont des fonctions entières à coefficients entiers de S, $[\varepsilon]$ est une unité quelconque de k ou une unité du corps K dont la puissance l^{eme} est une unité dans k; et enfin, ζ est une racine l^{me} de l'unité différente de 1.

Théorème 91. — Lorsque le degré relatif l du corps K cyclique relatif par rapport au corps k est un nombre premier impair, K possède un système de $r + 1$ unités relatives fondamentales, où r a par rapport à k le sens du théorème 47.

Démonstration. — Comme $l \neq 2$ parmi les lm corps conjugués déterminés par K, il y a lr_1 corps réels et lr_2 couples de corps imaginaires. Soient $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_r$ un système de $r = r_1 + r_2 - 1$ unités fondamentales du corps k. Choisissons parmi les unités de K une unité E_1, telle que $\mathsf{E}_1, \varepsilon_1, \dots, \varepsilon_r$ soit un système d'unités indépendantes; nous pouvons affirmer qu'alors

$$\mathsf{E}_1, \mathsf{E}_1^S, \dots, \mathsf{E}_1^{S^{l-2}}, \varepsilon_1, \dots, \varepsilon_r$$

forment un système d'unités indépendantes.

Pour le démontrer, supposons qu'il n'en soit pas ainsi et imaginons $\mathsf{E}_1^{F(S)} = \varepsilon^*$, où $F(S)$ est une fonction entière à coefficients entiers de degré $(l-2)$ qui n'est pas identiquement nulle et où ε^* est une unité du corps k. Comme la fonction $1 + S + \dots + S^{l-1}$ est irréductible (comparer à la remarque qui termine le § 91), on peut déterminer deux fonctions entières à coefficients entiers, G_1 et G_2 de S, et un nombre entier rationnel a différent de zéro, tels que

$$FG_1 + (1 + S + \dots + S^{l-1})G_2 = a.$$

Il en résulte, en tenant compte de

$$E_1^{(1-S)^{l-1}} = \varepsilon^{**},$$

que

$$E_1^l = \varepsilon^{***},$$

ce qui est contraire à l'hypothèse. Ici, ε^{**} et ε^{***} sont des unités de k.

Choisissons maintenant E_2 telles que $E_2, E_1, E_1^S, \ldots, E_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ forment un système d'unités indépendantes; nous montrerons, comme précédemment, qu'alors aussi les unités $E_2, E_2^S, \ldots, E_2^{S^{l-2}}, E_1, \ldots, E_1^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r$ forment un système d'unités indépendantes. En continuant ainsi, nous obtiendrons $r_1 + r_2 = r + 1$ unités $E_1, \ldots, E_{r+1}$, telles que les unités

$$E_i, E_i^S, \ldots, E_i^{S^{l-2}}, \varepsilon_1, \ldots, \varepsilon_r \qquad (i = 1, 2, \ldots, r+1)$$

forment un système d'unités indépendantes.

Le nombre de ces unités est

$$(r+1)(l-1) + r = lr_1 + lr_2 - 1.$$

Soit maintenant l^m une puissance assez élevée de l, pour que l'expression

$$(20) \qquad E_1^{F_1(S)} \cdots E_{r+1}^{F_{r+1}(S)} [\varepsilon]$$

où $F_1(S), \ldots, F_{r+1}(S)$ sont des fonctions entières à coefficients entiers quelconques de S et où $[\varepsilon]$ a le sens indiqué au début du paragraphe et ne puisse devenir la puissance d'exposant l^m d'une unité de K que si tous les coefficients des fonctions $F_1(S), \ldots, F_{r+1}(S)$ sont divisibles par l. On voit qu'un pareil exposant l^m existe si l'on considère les $lr_1 + lr_2 - 1$ unités du corps K données par le théorème 47.

Tenons compte maintenant de l'identité

$$(1-S)^l = 1 - S^l + lG(S)$$

où G est une fonction entière; comme d'après cela la $(1-S)^{l^m}$ème puissance symbolique d'un nombre de K est aussi une véritable puissance l^mème, il en résulte que l'expression (20) ne peut être la puissance symbolique d'exposant $(1-S)^{l^m}$ d'une unité que si tous les entiers algébriques $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ sont tous divisibles par $1-\zeta$.

Soit e_1 le plus grand nombre entier rationnel $\geqslant 0$, tel qu'une expression de la forme (20) soit une puissance symbolique d'exposant $(1-S)^{e_1}$ d'une unité, sans que tous les nombres $F_1(\zeta), \ldots, F_{r+1}(\zeta)$ soient tous divisibles par $1-\zeta$; admettons que

$$E_1^{F_1(S)} \cdots E_{r+1}^{F_{r+1}(S)} [\varepsilon] = H_1^{(1-S)^{e_1}}$$

soit une pareille expression où $F_1(S), \ldots, F_{r+1}(S)$ sont certaines fonctions entières rationnelles de S et où $F_1(S)$, par exemple, n'est pas divisible par $1-\zeta$; $[\varepsilon]$ a la signification précédente et H_1 est une certaine unité de K.

Admettons maintenant que e_2 est le plus grand entier $\geqq 0$ tel qu'il existe une expression correspondante formée des unités $\mathsf{E}_2, \ldots, \mathsf{E}_{r+1}$, qui soit la puissance symbolique de degré $(1-S)^{e_2}$ d'une unité de K, soit

$$\mathsf{E}_2^{F_2(S)} \ldots \mathsf{E}_{r+1}^{F_{r+1}(S)}[\zeta] = \mathsf{H}_2^{(1-S)^{e_2}},$$

où $F_2(S), \ldots, F_{r+1}(S)$ sont encore des fonctions rationnelles entières de S et où $F_2(\zeta)$, par exemple, n'est pas divisible par $1-\zeta$. En continuant ainsi, nous trouverons $r+1$ unités, $\mathsf{H}_1, \mathsf{H}_2, \ldots, \mathsf{H}_{r+1}$, qui forment un système d'unités relatives fondamentales de K.

Pour le démontrer, admettons qu'il n'en soit pas ainsi; il y aurait alors $r+1$ fonctions entières rationnelles $G_1(S), \ldots, G_{r+1}$, telles que

$$\mathsf{H}_1^{G_1(S)} \ldots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\zeta] = Z^{1-S},$$

où Z est une unité de K; soit, de plus, parmi les nombres $G_1(\zeta), \ldots, G_{r+1}(\zeta)$, par exemple $G_h(\zeta)$, le premier, qui n'est pas divisible par $1-\zeta$, il est évident que la seconde partie du dernier produit, c'est-à-dire

$$\mathsf{H}_h^{G_h(S)} \mathsf{H}_{h+1}^{G_{h+1}(S)} \ldots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\zeta]$$

serait aussi la puissance symbolique de degré $1-S$ d'une unité du corps K. Mais dans la suite des nombres $e_1, e_2, \ldots, e_{r+1}$ aucun ne dépasse le précédent; en élevant le dernier produit à la puissance $(1-S)^{e_h}$ et en introduisant les unités $\mathsf{E}_h, \ldots, \mathsf{E}_{r+1}$ nous nous heurterions à une contradiction.

Ce théorème 91 est vrai aussi pour $l=2$, comme on le voit facilement, si, parmi les $2m$ corps conjugués déterminés par K, il y a deux fois autant de corps réels que dans les m corps conjugués déterminés par k.

§ 56. — L'existence d'une unité de K, dont la norme relative est égale à 1 et qui cependant n'est pas le quotient de deux unités relatives conjuguées.

Théorème 92. — Dans le cas où le degré relatif l du corps cyclique relatif K par rapport à k est un nombre premier impair, il y a toujours dans K une unité H, dont la norme relative par rapport à k est égale à 1 et qui n'est pas la puissance symbolique de degré $(1-S)$ d'une unité du corps K.

Démonstration. — Admettons d'abord que le corps k ne contient pas la racine $l^{ième}$ de l'unité ζ. Soient $\eta_1, \ldots, \eta_{r+1}$, $r+1$ unités quelconques de k; il en résulte qu'il existe toujours $r+1$ entiers rationnels $a_1, \ldots, a_{r+1}$, qui ne sont pas tous divisibles par l et tels que $\eta_1^{a_1} \ldots \eta_{r+1}^{a_{r+1}} = 1$. En effet, si dans cette dernière égalité tous les exposants $a_1, \ldots, a_{r+1}$ étaient tous divisibles par l, $\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}}$ serait racine l^{me} de

l'unité, qui serait $= 1$ en vertu de l'hypothèse ; de là, par la répétition du procédé, résulte la démonstration. Si $\eta_1, \ldots, \eta_{r+1}$ sont les normes relatives des $H_1, \ldots, H_{r+1}$ unités fondamentales de k et que nous posions

$$H = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}},$$

il en résulte que

$$N_k(H) = H^{1+S+S^2+\ldots+S^{l-1}} = 1$$

et par suite, d'après le théorème 90, $H = A^{1-S}$; comme $H_1, \ldots, H_{r+1}$ sont des unités fondamentales relatives, il en résulte que A n'est pas une unité.

Pour démontrer le théorème 92 dans le cas général, nous admettrons que k contient la racine primitive $\sqrt[l^h]{1} = \zeta'$, mais qu'il ne contient pas la racine primitive d'indice l^{h+1}. On reconnaît, par un procédé analogue au précédent, que si $\eta_1, \ldots, \eta_{r+2}$ sont $r+2$ unités quelconques de k, on peut toujours trouver un nombre entier rationnel α et, de plus, $r+2$ entiers rationnels $a_1, \ldots, a_{r+2}$ non tous divisibles par l, tels que

$$\eta_1^{a_1} \ldots \eta_{r+2}^{a_{r+2}} = \zeta^{\alpha l}.$$

Considérons, d'autre part, que la norme relative

$$N_k(\zeta) = \zeta^{1+S+S^2+\ldots+S^{l-1}} = 1,$$

et que par conséquent, d'après le théorème 90, ζ doit être une puissance symbolique de degré $(1 - S)$. Si donc il n'y avait aucune unité E de k, telle que $\zeta = E^{1-S}$, ζ serait lui-même un nombre répondant à la question. Dans le cas contraire, il faut que $E^{l(1-S)} = 1$, c'est-à-dire $E^l = SE^l$, et, par suite, E^l serait une unité ε de k, tandis que E lui-même n'est pas dans k. Comme $E = \sqrt[l]{\varepsilon}$, on a $N_k(E) = E^l = \varepsilon$. Soit $H_1, \ldots, H_{r+1}$ un système d'unités relatives fondamentales dans k, nous poserons

$$\eta_1 = N_k(H_1), \quad \ldots, \quad \eta_{r+1} = N_k(H_{r+1}), \quad \eta_{r+2} = N_k(E) = E^l,$$

$$H = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}} E^{a_{r+2}} \zeta^{\alpha l - a} = H_1^{a_1} \ldots H_{r+1}^{a_{r+1}} [\varepsilon],$$

où $a, a_1, \ldots, a_{r+2}$ sont les nombres déterminés précédemment, et où $[\varepsilon]$ est la racine $l^{\text{ième}}$ d'une unité du corps k ; alors $N_k(H) = 1$. Les nombres $a_1, \ldots, a_{r+1}$ ne peuvent pas tous être divisibles par l. Car de

$$\left(\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}} E^{a_{r+2}} \zeta^{\alpha l - a}\right)^l = 1$$

on tirerait

$$\eta_1^{\frac{a_1}{l}} \ldots \eta_{r+1}^{\frac{a_{r+1}}{l}} E^{a_{r+2}} \zeta^{\alpha l - a} = \zeta^{b},$$

où b est un entier rationnel. Comme d'après notre hypothèse a_{r+2} ne peut pas aussi être divisible par l, il résulterait des dernières égalités que E est dans k, ce qui n'a pas lieu. L'unité H remplit toutes les conditions du théorème 92.

Les théorèmes 90, 91 et 92 ont été démontrés en partie et sous une autre forme par Kummer, dans le cas où le sous-corps k est le corps circulaire (Kreiskörper) de degré $l-1$ déterminé par ζ. [Kummer[14, 20, 21]].

§ 57. — Les idéaux ambiges et la différente relative du corps cyclique relatif K.

Lorsqu'un idéal $\mathfrak{A}$ du corps cyclique relatif reste inaltéré après la substitution S et qu'il ne contient aucun facteur qui soit un idéal de k, on dit que $\mathfrak{A}$ est un *idéal ambige*. En particulier, un idéal premier du corps K qui n'est pas altéré par la substitution S et qui n'appartient pas à k est dit un *idéal premier ambige*.

Théorème 93. — La différente du corps cyclique relatif K par rapport à k contient tous les idéaux premiers $\mathfrak{P}$ qui sont ambiges et elle n'en contient pas d'autres.

Démonstration. — Soit $\mathfrak{P}$ un idéal ambige; sa norme relative est $N_k(\mathfrak{P}) = \mathfrak{P}^l$. Comme k ne peut contenir une puissance inférieure de $\mathfrak{P}$, $\mathfrak{P}^l = \mathfrak{p}$ est un idéal premier de k. Réciproquement, si $\mathfrak{p}$ idéal premier de k est égal à la $l^{\text{ème}}$ puissance d'un idéal $\mathfrak{P}$ dans K, $\mathfrak{P}$ est un idéal premier ambige.

Nous distinguerons trois espèces d'idéaux premiers $\mathfrak{p}$ du corps k : d'abord, ceux qui sont égaux à la $l^{\text{ème}}$ puissance d'un idéal premier $\mathfrak{P}$ de K; deuxièmement, ceux qui dans K se décomposent en l idéaux premiers distincts de K, $\mathfrak{P}_1, \dots, \mathfrak{P}_l$; et enfin ceux qui sont aussi des idéaux premiers de K.

Dans le premier cas, la norme $N(\mathfrak{P}) = p^f$, d'où $N(\mathfrak{p}) = N(\mathfrak{P}^l) = p^{lf}$, et, par suite, la norme $n(\mathfrak{p})$ de l'idéal premier $\mathfrak{p}$ du corps k est aussi égale à p^f. L'égalité des normes permet d'affirmer que tout nombre entier de K est congru à un nombre entier de k suivant $\mathfrak{P}$; ceci permet de reconnaître que la différente relative de K par rapport à k est nécessairement divisible par $\mathfrak{P}$.

Dans le second cas, on peut toujours trouver dans K un entier A qui n'est pas divisible par $\mathfrak{P}_i$, mais qui l'est par tous les autres idéaux premiers $\mathfrak{P}_1, \dots, \mathfrak{P}_{i-1}, \mathfrak{P}_{i+1}, \dots, \mathfrak{P}_l$; c'est ce qui fait que la différente relative de A, et par suite celle du corps K, n'est pas divisible par $\mathfrak{P}_i$.

Pour ce qui concerne enfin les idéaux $\mathfrak{p}$ de la troisième espèce, soit P un nombre primitif suivant l'idéal premier $\mathfrak{p}$ de K et ρ un nombre primitif suivant $\mathfrak{p}$ dans k, et supposons aussi que P soit un nombre qui détermine le corps. P satisfait alors à une équation de degré l de la forme

$$F(\mathsf{P}) = \mathsf{P}^l + \alpha_1 \mathsf{P}^{l-1} + \dots + \alpha_l = 0,$$

dont les coefficients $\alpha_1, \dots, \alpha_l$ sont des nombres entiers de k.

Posons

$$\alpha_1 \equiv f_1(\rho), \;\dots,\; \alpha_l \equiv f_l(\rho) \pmod{\mathfrak{p}},$$

où $f_1(\rho), \dots, f_l(\rho)$ sont des fonctions entières à coefficients entiers de ρ. Nous obtiendrons la congruence

$$F(\mathsf{P}) = \mathsf{P}^l + f_1(\rho)\mathsf{P}^{l-1} + \dots + f_l(\rho) \equiv 0 \pmod{\mathfrak{p}}.$$

Comme $N(\mathfrak{p}) = (n(\mathfrak{p}))^l$, le nombre des entiers de K incongrus suivant $\mathfrak{p}$ est égal à la $l^{\text{ème}}$ puissance du nombre des entiers de k incongrus suivant $\mathfrak{p}$. P ne peut satisfaire à aucune congruence de même espèce et de degré inférieur à l, c'est-à-dire que $\dfrac{\partial F(\mathsf{P})}{\partial \mathsf{P}} \not\equiv 0$ suivant $\mathfrak{p}$, ou encore la différente relative du nombre P n'est pas divisible par $\mathfrak{p}$.

Ces considérations nous montrent que la différente relative du corps K est toujours un nombre premier avec les idéaux premiers de seconde et de troisième espèce, d'où le théorème 93.

§ 58. — Le théorème fondamental sur le corps cyclique relatif dont la différente relative est égale à 1. — On désigne ce corps le corps de classe.

Les théorèmes 90, 92, 93 nous apprennent un fait de très grande importance pour la théorie des corps de nombres. Ce fait s'énonce :

Théorème 94. — Lorsque le corps cyclique relatif K de degré premier impair l a par rapport à k sa différente relative égale à 1, il y a toujours dans k un idéal $\mathfrak{j}$, qui n'est pas un idéal principal de k, mais qui devient un idéal principal dans K. La $l^{\text{ème}}$ puissance de cet idéal $\mathfrak{j}$ est alors aussi nécessairement un idéal principal dans k et le nombre des classes du corps k est divisible par l.

Démonstration. — D'après le théorème 92, il y a une unité H de norme relative égale à 1 qui n'est pas la puissance de degré $(1 - S)$ d'une unité. D'après le théorème 90, $\mathsf{H} = \mathsf{A}^{1-S}$, où A est un nombre entier de K, c'est-à-dire que $\mathsf{A} = \mathsf{H}S(\mathsf{A})$. L'idéal principal $\mathfrak{A} = (\mathsf{A})$ est tel que $\mathfrak{A} = S\mathfrak{A}$. L'idéal $\mathfrak{A}$ fait partie du corps k. Car, soit $\mathfrak{P}$ un idéal premier de K contenu dans $\mathfrak{A}$, qui ne fait pas partie de k, le théorème 93, comme l'hypothèse nous montre que le discriminant relatif n'a pas de diviseur, montre que $\mathfrak{P} \neq S(\mathfrak{P})$ et, par suite, A contient aussi la norme relative $N_k(\mathfrak{P})$, qui est un idéal premier de k. L'idéal A n'est pas un idéal principal du corps k : car, dans ce cas, on aurait $\mathsf{A} = \mathsf{H}^*\alpha$, où H^* est une unité et α un nombre de k. Il en résulterait que $\mathsf{H} = \mathsf{H}^{*1-S}$, ce qui est contraire à ce qui précède. Ce qui démontre la première partie du théorème 94. Comme $N_k(\mathsf{A}) = \alpha$ est un nombre de k

et, par suite, $N_k(\mathfrak{A}) = \mathfrak{A}^l = (\alpha)$ est un idéal principal de k, nous avons la démonstration complète du théorème 94.

Les théorèmes 92 et 94 sont vrais aussi pour $l = 2$, si l'on fait la restriction indiquée à la fin du § 55.

Il n'y a pas de grandes difficultés de principe lorsqu'on veut étendre le théorème 94 à des corps abéliens relatifs K de différente relative égale à 1 et dont le degré relatif est un nombre composé.

Les rapports étroits du corps K avec certaines classses d'idéaux du corps k, mis à jour par le théorème 94, ont fait appeler ce corps K *un corps de classes du corps* k.

TROISIÈME PARTIE.

LE CORPS DE NOMBRES QUADRATIQUE.

CHAPITRE XVI.

La décomposition des nombres dans le corps quadratique.

§ 59. — La base et le discriminant du corps quadratique.

Soit m un entier rationnel positif ou négatif différent de 1, et qui n'est divisible par le carré d'aucun nombre autre que 1 ; l'équation du second degré

$$x^2 - m = 0$$

est irréductible dans le domaine des nombres rationnels.

Dans ce qui suit, nous désignerons par $\sqrt{m}$ la racine positive de cette équation lorsque $m > 0$ et lorsque $m < 0$ sa racine imaginaire positive. Le nombre algébrique $\sqrt{m}$ ainsi bien fixé détermine un corps réel ou imaginaire suivant les cas. Nous le désignerons par $k(\sqrt{m})$ ou, plus simplement, par k ; ce corps est toujours un corps de Galois. En remplaçant $+\sqrt{m}$ par $-\sqrt{m}$, on passe d'un nombre à son conjugué ou d'un idéal à son conjugué. Nous continuerons à employer la notation s pour indiquer cette transformation.

Le premier problème qui se présente à nous est la recherche d'une base du corps quadratique ainsi que de son discriminant. [Dedekind[1].]

Théorème 95. — Les nombres 1, ω, forment une base du corps quadratique k, si l'on pose

$$\omega = \frac{1+\sqrt{m}}{2} \quad \text{ou} \quad \omega = \sqrt{m}$$

suivant que $m \equiv 1\ (4)$ ou $m \not\equiv 1\ (4)$.

Le discriminant de k est, suivant les deux cas,

$$d = m, \qquad d = 4m.$$

Démonstration. — Le nombre ω est toujours un nombre entier, car il satisfait toujours soit à

$$x^2 - x - \frac{m-1}{4} = 0, \quad \text{soit à} \quad x^2 - m = 0, \tag{21}$$

soit $\omega' = s\omega$ le nombre conjugué de ω, le discriminant de ω est $d = (\omega - \omega')^2$. D'après le paragraphe 3, tout nombre entier du corps k est de la forme

$$\alpha = \frac{u + v\omega}{d},$$

où u, v sont des entiers rationnels.

Dans le cas où $m \equiv 1\,(4)$, la congruence $2\alpha m = 2u + v + v\sqrt{m} \equiv 0$ suivant m nous apprend que $2u + v$ est divisible par $\sqrt{m}$, et, par suite, $2u + v \equiv 0, (m)$. Cette dernière congruence, en tenant compte de la première $v\sqrt{m} \equiv 0, (m)$, c'est-à-dire que v est divisible par $\sqrt{m}$ et, par suite, par m. Les deux nombres u et v sont donc tous les deux divisibles par $d = m$, et l'on peut débarrasser le nombre α de son dénominateur.

D'autre part, soit $m \not\equiv 1\,(4)$, la congruence

$$4\alpha m = u + v\sqrt{m} \equiv 0, (m)$$

nous montre comme précédemment que u et v sont divisibles par m et que, par suite, m est contenu dans le numérateur et dans le dénominateur de l'expression qui donne α et qu'on peut simplifier par m.

Nous aurons donc $\alpha = \dfrac{u' + v'\sqrt{m}}{4}$ où u' et v' sont des entiers rationnels. Il est facile de voir, en formant la norme $\alpha . s\alpha$, que pour $m \equiv 2$, aussi bien que pour $m \equiv 3$ suivant 4, une expression de la forme $u' + v'\sqrt{m}$ avec u' et v' entiers et rationnels ne peut être divisible par 2 que si u' et v' sont tous les deux pairs. Si on applique ce résultat d'abord à 4α, puis à 2α, on voit que aussi dans le cas de $m \not\equiv 1\,(4)$ tout entier du corps k, s'écrit $u + v\omega$ avec u et v entiers et rationnels.

La seconde partie du théorème résulte de la formule

$$d = \begin{vmatrix} 1, & \omega' \\ 1, & \omega \end{vmatrix}^2 = (\omega - \omega')^2$$

qui, d'après le paragraphe 3, définit le discriminant du corps.

§ 60. — Les idéaux premiers du corps.

Le problème de la décomposition des nombres premiers rationnels en idéaux premiers du corps k est complètement résolu par le théorème suivant :

Théorème 96. — Tout nombre premier rationnel l facteur de d est le carré d'un

idéal premier de k. Tout nombre premier impair rationnel p qui ne divise pas d ou bien se décompose dans k en un produit de deux idéaux premiers conjugués du premier degré $\mathfrak{p}$ et $\mathfrak{p}'$ ou représente un idéal premier du second degré, suivant que d est reste quadratique de p ou non reste. Le nombre premier 2 est, dans le cas de $m \equiv 1 (4)$, le produit de deux idéaux conjugués distincts du premier degré de k, ou est lui-même un idéal premier suivant que $m \equiv 1$ ou $m \equiv 5$ suivant 8.

Démonstration. — La première partie de la proposition, celle qui a rapport aux facteurs premiers l de d, est une conséquence du théorème général 31. Soit l un facteur premier impair de d, nous trouvons

$$l = \mathfrak{l}^2,$$

où $\mathfrak{l} = (l, \sqrt{m})$ est un idéal premier du premier degré, qui est égal à son conjugué. Si 2 divise d, on a

$$2 = (2, \sqrt{m})^2 \quad \text{ou} \quad 2 = (2, 1 + \sqrt{m})^2$$

suivant que $m \equiv 2$ ou $m \equiv 3$ suivant 4.

La décomposition des nombres premiers non contenus dans d s'opère en tenant compte du théorème 33 et de la remarque qui s'y rapporte faite au paragraphe 13.

D'après ces considérations, tout nombre premier p qui ne divise pas d se décompose dans le corps k en deux idéaux premiers distincts ou est lui-même un idéal premier, suivant que le premier membre de l'équation correspondante (21) est réductible ou irréductible dans le sens de la congruence suivant p.

Si p est impair, nous trouvons que la congruence

$$(2x - 1)^2 - m \equiv 0 \quad \text{ou} \quad x^2 - m \equiv 0 \qquad (p)$$

n'est résoluble que si m est reste quadratique de p et qu'elle est irrésoluble si m est non-reste quadratique de p.

Posons dans le premier cas $m \equiv a^2$ suivant p; il vient

$$p = (p, a + \sqrt{m})(p, a - \sqrt{m}) = \mathfrak{p}.\mathfrak{p}'.$$

Les deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{p}'$ sont bien distincts à cause de

$$(p, a + \sqrt{m}, a - \sqrt{m}) = 1.$$

Dans le cas de $m \equiv 1 (4)$, la congruence $x^2 - x - \frac{m-1}{4} \equiv 0$ suivant 2 est évidemment résoluble ou irrésoluble suivant que $\frac{m-1}{4} \equiv 0$ ou $\equiv 1$ suivant 2, c'est-à-dire $m \equiv 1$ ou $\equiv 5$ suivant 8.

Dans le premier cas, on trouve

$$2 = \left(2, \frac{1 + \sqrt{m}}{2}\right)\left(2, \frac{1 - \sqrt{m}}{2}\right).$$

Les deux idéaux de droite sont différents, car

$$\left(2, \frac{1+\sqrt{m}}{2}, \frac{1-\sqrt{m}}{2}\right) = 1.$$

Nous pouvons prendre comme nombres de bases des idéaux que nous venons de trouver, soit

$$l, \frac{l+\sqrt{m}}{2} \quad \text{soit } l, \sqrt{m},$$

$$p, \frac{a \pm \sqrt{m}}{2} \quad \text{soit } p, a + \sqrt{m},$$

$$2, \frac{1 \pm \sqrt{m}}{2} \quad \text{soit } 2, \sqrt{m} \text{ ou } 2, 1+\sqrt{m},$$

suivant que $m \equiv 2, 3 (4)$.

On reconnaît facilement ce fait par une réciproque du théorème 19, si l'on forme le déterminant obtenu en adjoignant à chacun de ces couples de nombres le couple conjugué. Dans la deuxième ligne du petit tableau que l'on vient d'établir, a désigne un nombre satisfaisant à la congruence

$$a^2 \equiv m \qquad (p)$$

et qui, de plus, est supposé impair dans le cas de $m \equiv 1 (4)$.

§ 61. — Le symbole $\left(\frac{a}{w}\right)$.

Pour pouvoir donner un énoncé résumé et complet des résultats acquis, nous introduirons le symbole suivant : Soit a un entier quelconque rationnel et w un nombre premier rationnel impair, le *symbole* $\left(\frac{a}{w}\right)$ a la valeur $+1$, -1 ou 0 suivant que a est reste quadratique ou non-reste quadratique de p ou qu'il est divisible par p; de plus, admettons que $\left(\frac{a}{2}\right)$ égale $+1$, -1 ou 0 suivant que a impair est reste quadratique ou non-reste de $2^3 = 8$, ou suivant qu'il est divisible par 2.

On peut alors donner au théorème 96 l'énoncé

Théorème 97. — Un nombre premier rationnel quelconque $p (= 2$ ou $\neq 2)$ se décompose dans le corps k en deux idéaux premiers distincts, est lui-même un idéal premier, ou est le carré d'un idéal premier suivant que

$$\left(\frac{d}{p}\right) = +1, -1 \quad \text{ou} \quad 0. \qquad \text{[Dedekind [1].]}$$

Ceci nous amène à considérer trois espèces d'idéaux premiers :

1° Les idéaux premiers du premier degré $\mathfrak{p}$ distincts de leurs conjugués $\mathfrak{p}'$.

2° Les idéaux du second degré (p) représentés par les nombres premiers qui ne se décomposent pas dans k.

3° Les idéaux du premier degré $\mathfrak{l}$ dont les carrés sont des nombres premiers contenus dans d.

D'après les définitions des paragraphes 39 et 41, le corps k est le corps de décomposition des idéaux premiers p de la première espèce, il est le corps d'inertie pour les idéaux premiers p de la seconde espèce et enfin le corps de ramification pour les idéaux $\mathfrak{l}$ de la troisième espèce.

§ 62. — Les unités du corps quadratique.

Pour ce qui concerne les unités de k, le théorème 47 nous apprend que nous avons à considérer deux cas, suivant que k est un corps imaginaire ou un corps réel.

Dans le premier cas, k ne peut contenir d'autres unités que celles qui sont des racines de l'unité, et comme le corps quadratique ne peut contenir que les racines primitives de la racine cubique, quatrième ou sixième de l'unité, les seuls corps quadratiques imaginaires qui peuvent contenir d'autres unités que -1 et $+1$ sont les deux corps $k(\sqrt{-1})$ et $k(\sqrt{-3})$. Le premier corps contient les unités $\pm i$; le second, les quatres unités $\pm \frac{1 \pm \sqrt{-3}}{2}$. Les discriminants de ces deux corps sont -4 et -3; d'après le théorème 50, il y a dans toute classe d'idéaux de ces corps un idéal dont la norme $\leqq 2$ pour le premier, $\leqq \sqrt{3}$ pour le second. Comme d'ailleurs dans le corps $k(\sqrt{-1})$, le nombre 2 est la norme de l'idéal principal $(1+i)$; il en résulte que chacun de ces deux corps ne possède qu'une classe d'idéaux. Ces corps ne renferment donc que des idéaux principaux, et tout nombre positif entier rationnel qui peut être pris pour norme d'un idéal de $k(\sqrt{-1})$ ou de $k(\sqrt{-3})$ est aussi la norme d'un entier algébrique dans le corps correspondant, d'où résultent les théorèmes connus sur la représentation des entiers rationnels sous les formes $x^2 + y^2$ ou $x^2 + xy + y^2$, x et y étant des entiers rationnels.

Par contre, si k est un corps réel, le théorème 47 nous apprend qu'il existe toujours une unité fondamentale ε différente de -1, et au moyen de laquelle toute unité du corps peut être mise d'une seule façon sous la forme $\pm \varepsilon^a$, où a est un entier rationnel.

Les circonstances dans lesquelles la norme de cette unité fondamentale est égale à $+1$ ou à -1 n'ont été découvertes que dans certains cas particuliers. [Arndt[1], Dirichlet[4], Legendre[1], Tano[1].] — Comparez à ce que nous venons de dire la première partie de la démonstration du lemme 13.

§ 63. — Les classes d'idéaux.

Les calculs du paragraphe 24 permettent d'établir toutes les classes d'idéaux du corps quadratique k pour chaque valeur particulière de m. Il a été construit des tables basées sur la théorie des formes quadratiques réduites et qu'il faudrait citer ici. [Gauss[1], Cayley[1].]

CHAPITRE XVII.

Les genres dans le corps quadratique et leurs systèmes de caractères.

§ 64. — Le symbole $\left(\frac{n, m}{w}\right)$.

Pour la répartition des classes d'idéaux, nous introduirons dans les développements de la théorie du corps quadratique un nouveau symbole. Soient n et m deux entiers rationnels, où m n'est pas un carré et où w est un nombre premier rationnel quelconque; nous donnerons au symbole $\left(\frac{n, m}{w}\right)$ la valeur $+1$, dès que le nombre n est congru à la norme d'un entier du corps algébrique $k(\sqrt{m})$, et si, de plus, il existe pour toute puissance plus élevée de w dans $k(\sqrt{m})$ un nombre entier dont la norme est congrue à n suivant cette puissance de w; dans tout autre cas, nous poserons $\left(\frac{n, m}{w}\right) = -1$. Les nombres pour lesquels $\left(\frac{n, m}{w}\right) = +1$ seront dits les restes normiques du corps $k(\sqrt{m})$ suivant w; les nombres n pour lesquels $\left(\frac{n, m}{w}\right) = -1$ seront les *non-restes* normiques du corps $k(\sqrt{m})$ suivant w.

Lorsque m est carré parfait, $\left(\frac{n, m}{w}\right)$ sera toujours pris égal à $+1$.

Le théorème suivant nous indique les propriétés du symbole $\left(\frac{n, m}{w}\right)$ qui nous permettront de le calculer.

Théorème 98. — Soient n et m deux entiers rationnels, qui ne sont pas divisibles par w, on a les règles suivantes :

Pour les nombres premiers impairs w, on a :

$$(a') \qquad \left(\frac{n,\, m}{w}\right) = +1,$$

$$(a'') \qquad \left(\frac{n,\, w}{w}\right) = \left(\frac{w,\, n}{w}\right) = \left(\frac{w}{n}\right);$$

pour $w = 2$:

$$(b') \qquad \left(\frac{n,\, m}{2}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}};$$

$$(b'') \qquad \left(\frac{n,\, 2}{2}\right) = \left(\frac{2,\, n}{2}\right) = (-1)^{\frac{n^2-1}{8}}.$$

De plus, pour des nombres entiers rationnels quelconques n, n', m, m' par rapport à tout nombre premier w, on a les formules

$$(c') \qquad \left(\frac{-m,\, n}{w}\right) = +1,$$

$$(c'') \qquad \left(\frac{n,\, m}{w}\right) = \left(\frac{m,\, n}{w}\right),$$

$$(c''') \qquad \left(\frac{nn',\, m}{w}\right) = \left(\frac{n,\, m}{w}\right)\left(\frac{n',\, m}{w}\right),$$

$$(c'''') \qquad \left(\frac{n,\, mm'}{w}\right) = \left(\frac{n,\, m}{w}\right)\left(\frac{n,\, m'}{w}\right).$$

Démonstration. — D'abord il est évident que si n est la norme d'un entier de k, on a $\left(\frac{n,\, m}{w}\right) = +1$.

De plus, comme $-m$ est la norme de $\sqrt{m}$, on en conclut l'exactitude de (c'). De plus, si n et n' sont deux entiers rationnels $\neq 0$, dont le quotient est la norme d'un entier ou d'une fraction de $k(\sqrt{m})$, l'égalité

$$\left(\frac{n,\, m}{w}\right) = \left(\frac{n',\, m}{w}\right)$$

est évidente d'après la définition du symbole.

Si $\frac{n}{n'}$ est le carré d'un nombre rationnel, il en résulte en particulier ce fait très simple que la valeur du symbole $\left(\frac{n,\, m}{w}\right)$ ne change pas si l'on multiplie n ou si on le divise par le carré d'un nombre rationnel entier. Nous admettrons, pour plus de simplicité, que ni n ni m ne contienne le carré d'un nombre premier.

Pour reconnaître l'exactitude de notre système de formules, nous traiterons dans l'ordre les trois cas particuliers suivants :

1) Soit w un nombre premier impair qui divise m.

Si n n'est pas aussi divisible par w, la congruence

$$(22) \qquad 4n \equiv (2x - y)^2 - my^2 \quad \text{ou} \quad n \equiv x^2 - my^2 \quad (w),$$

n'admet de solution entière en x et y que si $\left(\frac{n}{w}\right) = +1$. Réciproquement, si la dernière condition est satisfaite, la congruence $n^2 \equiv x^2$ admet des solutions suivant toutes les puissances de w, et il en est évidemment de même de la congruence (22). Donc, en vertu des hypothèses admises,

$$\left(\frac{n,\, m}{w}\right) = \left(\frac{n}{w}\right).$$

D'autre part, si n est divisible par w,

$$\left(\frac{n,\, m}{w}\right) = \left(\frac{-nm,\, m}{w}\right) = \left(\frac{\frac{-nm}{w^2}\,.\,m}{w}\right) = \left(\frac{\frac{-nm}{w^2}}{w}\right).$$

2) Soit w un nombre premier impair qui ne divise pas m. Si n aussi n'est pas divisible par w, la congruence

$$n \equiv x^2 - my^2 \quad (w)$$

admet toujours des solutions, car le second membre de cette congruence donne tous les restes quadratiques suivant w, lorsqu'on fait $x = 1, 2, \ldots, \frac{w-1}{2}$, $y = 0$; et, dans le cas de $\left(\frac{-m}{w}\right) = -1$, elle donne tous les restes non quadratiques suivant w, pour $x = 0$, $y = 1, 2, \ldots, \frac{w-1}{2}$.

Par contre, soit $\left(\frac{-m}{w}\right) = +1$, désignons par a le plus petit non-reste quadratique du nombre premier w, et soit $y = b$ une racine de la congruence $-my^2 \equiv a - 1\ (w)$ qui a certainement des solutions; comme $a \equiv 1 - mb^2$ suivant w, la forme $x^2 - m(bx)^2$ représente pour $x = 1, 2, \ldots, \frac{w-1}{2}$ tous les non-restes quadratiques suivant w.

Comme la congruence $n \equiv x^2 - my^2$ suivant w admet des solutions, on en conclut qu'elle en admet aussi suivant toutes les puissances de w, c'est-à-dire qu'avec nos hypothèses

$$\left(\frac{n,\, m}{w}\right) = +1.$$

Admettons maintenant que n est divisible par w, mais qu'il ne l'est pas par w^2; conformément aux hypothèses du début, une solution de $n \equiv x^2 - my^2$ suivant w^2 :

$$\chi = x - \sqrt{m}\, y$$

représenterait un nombre du corps $k(\sqrt{m})$, dont la norme $\xi . s\xi = n(\xi)$ contiendrait en facteur w et non pas w^2, c'est-à-dire que w se décomposerait dans le corps $k(\sqrt{m})$ en deux idéaux premiers distincts $\mathfrak{w}$ et $\mathfrak{w}'$, ce qui exige comme condition nécessaire et suffisante, d'après le théorème 97, $\left(\frac{m}{w}\right) = +1$.

Réciproquement donc, si cette condition est remplie, w est dans le corps $k(\sqrt{m})$ un produit $\mathfrak{w}\mathfrak{w}'$ de deux idéaux premiers distincts. Si l'on désigne alors par α un nombre entier de $k(\sqrt{m})$ divisible par $\mathfrak{w}$, mais non par $\mathfrak{w}^2$ ou par $\mathfrak{w}'$,

$$\left(\frac{n, m}{w}\right) = \left(\frac{n . n(\alpha), m}{w}\right) = \left(\frac{\frac{n . n(\alpha)}{w^2}, m}{w}\right) = +1,$$

c'est-à-dire qu'avec les hypothèses actuelles, on a toujours $\left(\frac{n, m}{w}\right) = \left(\frac{m}{w}\right)$.

Les résultats acquis établissent immédiatement l'exactitude des formules (a') et (a''); de plus, ils donnent pour des nombres premiers impairs les formules (c') et (c''), et ils les donnent complètement si l'on examine dans l'ordre les différents cas qui peuvent se présenter en tenant compte de la divisibilité ou de la non-divisibilité des nombres n, n', m par w.

3) Dans le cas de $w = 2$, nous ferons d'abord les considérations suivantes. Soit $f(xy)$ une fonction homogène du second degré à coefficients entiers de x et de y, et n un nombre entier rationnel impair; si la congruence $n \equiv f(xy)$ suivant 2^3 admet des racines, elle en admet aussi suivant toute puissance supérieure de 2, 2^{e+1} $(e \geqq 3)$. Nous le démontrerons en concluant de e à $e+1$. Soient a, b deux entiers rationnels, tels que $f(a, b) \equiv n$ suivant 2e, où $e \geqq 3$; si l'on n'a pas $n \equiv f(a, b)$ suivant 2^{e+1}, mais bien mieux $n \equiv f(a, b) + 2^e$ suivant 2^{e+1}, nous déterminerons un nombre c, tel que $c^2 \equiv 1 + 2^e$ suivant 2^{e+1}, ce qui est possible à cause de $e > 2$; et alors

$$f(ca, cb) = c^2 f(a, b) \equiv f(a, b) + 2^e f(a, b) \equiv f(a, b) + 2^e \equiv n \quad (2^{e+1});$$

c'est ce que nous voulions démontrer.

Dès lors, si nous voulons établir la valeur de $\left(\frac{n, m}{2}\right)$ pour n impair, il nous faut chercher quelles sont les valeurs de n et de m qui se correspondent de manière à rendre possibles les congruences

$$(23) \qquad \underset{(m \equiv 1, 4)}{n \equiv x^2 + xy - \frac{m-1}{4} y^2} \quad \text{ou} \quad \underset{(m \equiv 2, 3 (4))}{n \equiv x^2 - m y^2} \quad (2^4).$$

Un calcul très court nous fournit la table suivante :

Dans cette table, nous avons mis dans la colonne des m les six restes suivant 2^3 à considérer, et, dans la colonne des n, les restes impairs suivant 2^3 qui leur correspondent et rendent possible la congruence 23 :

m	n
1	1, 3, 5, 7
2	1, 7
3	1, 5
5	1, 3, 5, 7
6	1, 3
7	1, 5

Cette table nous montre que pour n et m impairs l'égalité (b') est vraie ; elle montre aussi que pour n impair, m pair $= 2m'$; on a :

$$\left(\frac{n\,,\,2m'}{2}\right)=(-1)^{\frac{n^2-1}{8}+\frac{n-1}{2}\cdot\frac{m'-1}{2}}.$$

D'autre part, si n est pair $= 2n'$ et m impair, il faut distinguer les deux cas $m \equiv 1$ et $m \equiv 3$ suivant 4.

Dans le premier cas, il faut que 2 soit dans le corps $k(\sqrt{m})$ le produit de deux idéaux premiers distincts dès que $n = 2n'$ est reste normique de 2 dans $k(\sqrt{m})$, c'est-à-dire que $\left(\frac{m}{2}\right)$ doit être égal à $+1$. Si cette condition est remplie, on peut toujours trouver un nombre α dans $k(\sqrt{m})$ dont la norme $n(\alpha)$ est divisible par 2 et non par 4 ; on a alors

$$\left(\frac{2n'\,,\,m}{2}\right)=\left(\frac{2n'\,.\,n(\alpha)\,,\,m}{2}\right)=\left(\frac{\frac{n'\,.\,n(\alpha)}{2}\,,\,m}{2}\right),$$

et ce dernier symbole suivant (b') est égal à -1 ; on a donc

$$\left(\frac{2n'\,,\,m}{2}\right)=-\left(\frac{m}{2}\right)=-(-1)^{\frac{m^2-1}{8}}.$$

Dans l'autre cas $m \equiv 3 (4)$, la valeur du symbole en question dépend de la possibilité de la congruence $2n' \equiv x^2 - my^2$ suivant une puissance quelconque de 2. Une pareille congruence, comme on le voit aisément, n'est possible que s'il en est ainsi de

$$m \equiv x^2 - 2n'y^2$$

suivant la même puissance 2e; c'est-à-dire que

$$\left(\frac{2n',\ m}{2}\right) = \left(\frac{m,\ 2n'}{2}\right).$$

Enfin, si n et m sont tous les deux divisibles par 2, $n = 2n'$, $m = 2m'$, on a

$$\left(\frac{2n',\ 2m'}{2}\right) = \left(\frac{-2^2 n'm',\ 2m'}{2}\right) = \left(\frac{-n'm',\ 2m'}{2}\right).$$

Les résultats obtenus ont pour conséquence immédiate la formule (b''), et nous reconnaissons en même temps que les formules (c'') et (c''') sont exactes pour $w = 2$. La formule c'''' se déduit d'une combinaison de (c'') et (c''').

Le théorème 98 est complètement démontré.

Des formules (a'), (a''), (b'), (b'') du théorème 98, on déduit ce qui suit :

Si l'on considère un système complet de nombres premiers avec w et incongrus suivant w^e, où $e \geqq 1$ et même $e > 2$ dans le cas de $w = 2$, tous ces nombres sont des restes normiques du corps $k(\sqrt{m})$ suivant m, ou bien ils forment la moitié de ces restes, suivant que w est premier avec le discriminant de $k(\sqrt{m})$ ou qu'il ne l'est pas.

§ 65. — Les systèmes de caractères d'un idéal.

Soit t le nombre des diviseurs premiers rationnels des discriminants de $k(\sqrt{m})$, désignons-les par $l_1, l_2, \dots, l_t$.

A chaque nombre entier rationnel correspondent alors des valeurs parfaitement déterminées ($+1$ ou -1) des t symboles

$$\left(\frac{a,\ m}{l_1}\right), \dots, \left(\frac{a,\ m}{l_t}\right)$$

dont le sens est déterminé par le paragraphe précédent; ces t unités ± 1 prendront le nom de système des caractères du nombre a dans le corps $k(\sqrt{m})$. Pour pouvoir attribuer aussi à tout idéal $\mathfrak{a}$ du corps $k(\sqrt{m})$ un système de caractères bien déterminé, nous distinguerons deux cas suivant que k est un corps imaginaire ou un corps réel. Dans le premier cas, les normes des nombres de $k(\sqrt{m})$ sont toujours positives; nous poserons $r = t$, $n = n(\mathfrak{a})$, et nous dirons que les r unités

(24) $$\left(\frac{n,\ m}{l_1}\right), \dots, \left(\frac{n,\ m}{l_r}\right)$$

forment le système des caractères de l'idéal $\mathfrak{a}$, il est parfaitement déterminé par l'idéal $\mathfrak{a}$. Dans le second cas, nous formerons d'abord le système des caractères du nombre -1 :

$$(25) \qquad \left(\frac{-1,\, m}{l}\right), \;\ldots,\; \left(\frac{-1,\, m}{l_t}\right).$$

Si toutes ces unités sont égales à $+1$, nous poserons, comme dans le premier cas, $n = n(\mathfrak{a})$, $r = t$, et nous dirons encore que le système (24) est le système des caractères de $\mathfrak{a}$. Par contre, si parmi les t caractères (25) se trouve l'unité -1, soit par exemple $\left(\frac{-1,\, m}{l_t}\right) = -1$, nous poserons $r = t - 1$ et $\bar{n} = \pm n(\mathfrak{a})$ en choisissant le signe de façon que $\left(\frac{\bar{n},\, m}{l_t}\right) = +1$, et nous désignerons les r unités (24) résultant de ces hypothèses sur r et sur $\bar{n}$ le système des caractères de l'idéal $\mathfrak{a}$.

Les conventions que nous venons de faire nous permettent d'énoncer le théorème suivant :

§ 66. — Le système de caractères d'une classe d'idéaux et la notion de genre.

Théorème 99. — Tous les idéaux d'une même classe du corps $k(\sqrt{m})$ admettent le même système de caractères.

Démonstration. — Soient $\mathfrak{a}$ et $\mathfrak{a}'$ deux idéaux de $k(\sqrt{m})$ appartenant à la même classe ; il existe un nombre α entier ou fractionnaire de $k(\sqrt{m})$, tel que $\mathfrak{a}' = \alpha\mathfrak{a}$. Par suite, $n(\mathfrak{a}') = \pm n(\alpha) n(\mathfrak{a})$, où $\pm$ désigne le signe de $n(\alpha)$, et, par suite,

$$\left(\frac{n(\mathfrak{a}'),\, m}{l}\right) = \left(\frac{\pm n(\mathfrak{a}),\, m}{l}\right)$$

pour $l = l_1, \ldots, l_t$. En tenant compte des conventions du paragraphe 65, on obtient le théorème 99.

De cette façon, à chaque classe d'idéaux correspond un système de caractères. Nous rangerons dans le même *genre* toutes les classes d'idéaux qui ont le même système de caractères, et, en particulier, nous définirons genre principal l'ensemble de toutes les classes dont les systèmes de caractères est formé d'unités toutes positives. Comme le système de caractères de la classe principale a évidemment cette propriété, la classe principale appartient au genre principal. De la formule c'', paragraphe 64, nous déduirons facilement ce fait, que la multiplication des classes d'idéaux de deux genres fournit la classe d'idéaux d'un genre, dont le système de caractères s'obtient par la multiplication des caractères correspondants des deux genres. Il en résulte en particulier que le système des caractères du carré d'une classe d'idéaux d'un genre quelconque ne contient que des unités positives, et, par suite, le carré de toute classe d'idéaux appartient au genre principal.

Tout genre contient le même nombre de classes.

§ 67. — Théorème fondamental relatif aux genres du corps quadratique.

Une question se pose : Un système quelconque de r unités ± 1 peut-il être le système de caractères d'un genre du corps $k(\sqrt{m})$? La solution de cette question est d'une importance capitale pour la théorie du corps quadratique; elle est contenue dans un théorème dont la démonstration nous occupera jusqu'au paragraphe 78 et qui s'énonce :

Théorème 100. — La condition nécessaire et suffisante pour qu'un système quelconque de r unités ± 1 soit le système des caractères d'un genre du corps $k(\sqrt{m})$ est que le produit des r unités soit égal à $+1$. C'est pourquoi le nombre des genres du corps $k(\sqrt{m})$ est égal à 2^{r-1}. [Gauss[1].]

§ 68. — Un lemme s'appliquant aux corps quadratiques dont le discriminant ne contient qu'un diviseur premier.

Pour nous rapprocher du but indiqué au théorème 100, nous démontrerons d'abord le

Lemme 13. — Lorsque le discriminant d'un corps $k = k(\sqrt{m})$ ne contient qu'un diviseur premier rationnel l, le nombre des classes d'idéaux de k est impair. Le système des caractères se compose d'un caractère unique relatif à l; ce caractère est toujours égal à $+1$, c'est-à-dire que dans le corps il n'y a qu'un genre : le genre principal.

Démonstration. — Désignons par s la substitution qui transforme un nombre du corps k en son conjugué. Désignons encore, lorsque $m > 0$, par ε une unité fondamentale du corps k, $-\varepsilon$, $\frac{1}{\varepsilon}$, $-\frac{1}{\varepsilon}$ représentent des unités du même genre; nous démontrerons tout d'abord que l'hypothèse du lemme nous donne $n(\varepsilon) = \varepsilon \,.\, s\varepsilon = -1$. En effet, admettons que $n(\varepsilon) = +1$, on pourrait trouver, d'après le théorème 90, un entier α du corps tel que $\varepsilon = \frac{\alpha}{s(\alpha)}$; il en résulte $\alpha = \varepsilon \,.\, s\alpha$, c'est-à-dire que tout facteur idéal premier contenu dans α le serait dans $s\alpha$. Mais d'après l'hypothèse faite dans l'énoncé, lorsque $m > 0$ $\sqrt{m}$ est le seul facteur premier de k, qui est égal à son conjugué et qui n'est pas rationnel, on a ou bien

$$\alpha = \eta_1 a \qquad \text{ou} \qquad \alpha = \eta_1 \sqrt{m}\, a,$$

η_1 étant une unité et a un entier rationnel positif ou négatif; il en résulterait $\varepsilon = \pm \eta_1^{1-s} = \pm \eta_1^2$, et ε ne serait pas une unité fondamentale, ce qui est contraire à l'hypothèse.

Démontrons maintenant la première partie du lemme. Si le nombre h des classes du corps k était pair, il y aurait, suivant le théorème 57, un idéal $\mathfrak{j}$ n'appartenant pas à la classe principale, tel que $\mathfrak{j}^2 \sim 1$; mais comme $\mathfrak{j}s\mathfrak{j} \sim 1$, on en conclurait $\mathfrak{j} \sim s\mathfrak{j}$. Posons $\mathfrak{j} = \alpha s.\mathfrak{j}$, c'est-à-dire $\mathfrak{j}^{1-s} = \alpha$; α est un nombre de k dont la norme $n(\alpha) = \pm 1$. Dans le cas où le signe serait $+$, posons $\beta = \alpha$; le second n'est évidemment possible que pour un corps réel; faisons $\beta = \varepsilon\alpha$, ε désignant comme tout à l'heure l'unité fondamentale de k. Avec ces hypothèses, on aurait à chaque fois $n(\beta) = +1$, et, par suite, d'après le théorème 90, $\frac{1}{\beta} = \gamma^{1-s}$, où γ est un entier de k. De $\alpha = \mathfrak{j}^{1-s}$ résulterait $(\gamma\mathfrak{j})^{1-s} = 1$, c'est-à-dire $(\gamma)\mathfrak{j} = s(\gamma\mathfrak{j})$, et on conclurait comme précédemment que l'idéal $(\gamma)\mathfrak{j}$ est ou bien $= (a)$ ou $(a)\mathfrak{l}$, où a est un nombre entier rationnel et $\mathfrak{l}$ le seul nombre premier de k égal à son conjugué et non rationnel. Or, lorsque $m \neq -1$, ce facteur premier $\mathfrak{l} = \sqrt{m}$, et, pour $m = -1$, $\mathfrak{l} = 1 + \sqrt{-1}$, c'est-à-dire qu'on a toujours $\mathfrak{l} \sim 1$, et, par suite, $\mathfrak{j} \sim 1$, ce qui est contraire à l'hypothèse.

Lorsque k est un corps réel, $n(\varepsilon) = -1$ nous indique de suite que

$$\left(\frac{-1, m}{l}\right) = +1,$$

et alors, d'après le paragraphe 65, le système du caractère d'un idéal $\mathfrak{j}$ est constitué par l'unité $\left(\frac{\pm n(\mathfrak{j}), m}{l}\right)$; ce caractère unique est égal à $+1$ pour chaque idéal $\mathfrak{j}$ du corps k, sans quoi l'ensemble des classes d'idéaux de k se répartirait en deux genres et le nombre des classes h serait pair.

Ce lemme 13 nous montre que le théorème fondamental 100 est vrai dans le cas le plus simple, c'est-à-dire le cas du corps quadratique dont le discriminant d ne contient qu'un diviseur premier rationnel.

§ 69. Le théorème de réciprocité pour les restes quadratiques. Un lemme relatif au symbole $\left(\frac{n, m}{w}\right)$.

Théorème 101. — Soit p et q deux nombres premiers rationnels impairs positifs différents l'un de l'autre; on a la règle

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

dite loi de réciprocité des restes quadratiques. On a, de plus,

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

dits théorèmes complémentaires à la loi de réciprocité quadratique. [Gauss[1].]

Démonstration. — Soit $k(\sqrt{m})$ un corps dont le discriminant ne contient qu'un diviseur premier l, et désignons par n la norme d'un idéal de ce corps k ; d'après le lemme 13 on a toujours $\left(\frac{n, m}{l}\right) = -1$. Mais d'après les théorèmes 96 et 97, on voit, qu'en particulier, tout nombre premier positif impair qui ne divise pas m et dont m est reste quadratique est la norme d'un idéal de $k(\sqrt{m})$. Nous utiliserons ce fait pour dresser le tableau suivant : nous désignerons par p et p' deux nombres premiers rationnels distincts congrus à 1 suivant 4, par q et q' deux nombres premiers distincts congrus à 3 suivant 4, tandis que r représentera un nombre premier rationnel impair dont nous ne préjugeons pas le reste par 4.

	Si :				On a :
	m	l	n	$\left(\frac{m}{n}\right) = +1$	$\left(\frac{n, m}{l}\right) = -1$
1.	-1	2	r	$\left(\frac{-1}{r}\right) = -1$	$\left(\frac{r, -1}{2}\right) = (-1)^{\frac{r-1}{2}} = -1$
2.	2	2	r	$\left(\frac{2}{r}\right) = +1$	$\left(\frac{r, 2}{2}\right) = (-1)^{\frac{r^2-1}{8}} = -1$
3.	p	p	p'	$\left(\frac{p}{p'}\right) = -1$	$\left(\frac{p', p}{p}\right) = \left(\frac{p'}{p}\right) = -1$
4.	p	p	q	$\left(\frac{p}{q}\right) = -1$	$\left(\frac{q, p}{p}\right) = \left(\frac{q}{p}\right) = -1$
5.	$-q$	q	p	$\left(\frac{-q}{p}\right) = +1$	$\left(\frac{p, -q}{q}\right) = \left(\frac{p}{q}\right) = -1$
6.	$-q$	q	q'	$\left(\frac{-q}{q'}\right) = +1$	$\left(\frac{q', -q}{q}\right) = \left(\frac{q'}{q}\right) = +1$

Dans un corps $k(\sqrt{p})$, $n(\varepsilon) = -1$ nous apprend que $\left(\frac{-1}{p}\right) = -1$; ajoutons cette remarque à la ligne 1, il en résulte que, d'une façon générale, $\left(\frac{-1}{r}\right) = (-1)^{\frac{r-1}{2}}$.

Appliquons la proposition citée au début de cette démonstration au nombre premier $n = 2$, et remarquant que 2 est toujours la norme d'un idéal dans $k(\sqrt{p})$, ou $k(\sqrt{-q})$, dès que $(-1)^{\frac{p^2-1}{8}} = +1$ ou $(-1)^{\frac{q^2-1}{8}} = -1$, il en résulte que, si ces conditions sont satisfaites, $\left(\frac{2, p}{p}\right) = \left(\frac{2}{p}\right) = -1$, ou $\left(\frac{2, -q}{q}\right) = \left(\frac{2}{q}\right) = +1$, c'est-à-dire que si $(-1)^{\frac{r^2-1}{8}} = +1$, on a $\left(\frac{2}{r}\right) = -1$. Ajoutons ce résultat à la ligne 2, on a, d'une façon générale, $\left(\frac{2}{r}\right) = (-1)^{\frac{r^2-1}{8}}$. Le contenu de la ligne 3 montre que $\left(\frac{p}{p'}\right) = \left(\frac{p'}{p}\right)$.

Les lignes 4 et 5 nous apprennent que

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$$

et la ligne 6 que $\left(\frac{q}{q'}\right) = -\left(\frac{q'}{q}\right)$, où il faut tenir compte du caractère du reste de -1, qui a été trouvé d'abord.

Il reste à démontrer que si $\left(\frac{q}{q'}\right) = +1$, on a nécessairement $\left(\frac{q'}{q}\right) = -1$. Le théorème de réciprocité pour deux nombres premiers rationnels q et q', qui tous deux $\equiv 3$ suivant (4), s'obtient le plus simplement en considérant le corps $k(\sqrt{qq'})$, car comme $\left(\frac{-1, qq'}{q}\right) = -1$, la norme de l'unité fondamentale ε de ce corps est certainement $= +1$, et il y a un entier α (voir théorème 90), tel que $\varepsilon = \alpha^{1-S} = \frac{\alpha}{S\alpha}$, où $S\alpha$ est le nombre conjugué de α. Nous en conclurons facilement que l'idéal premier $\mathfrak{q}$ contenu dans q est un idéal principal. Par suite, en choisissant convenablement le signe,

$$\left(\frac{\pm q, qq'}{q}\right) = +1 \quad \text{et} \quad \left(\frac{\pm q, qq'}{q'}\right) = +1;$$

donc

$$\left(\frac{q, qq'}{q}\right) = \left(\frac{q, qq'}{q'}\right);$$

et en tenant compte de la formule (c') du théorème 98 :

$$-\left(\frac{q'}{q}\right) = \left(\frac{q}{q'}\right).$$

Lemme 14. — Soient n et m deux entiers rationnels quelconques qui ne sont pas tous deux négatifs; on a

$$\prod_{(w)} \left(\frac{n, m}{w}\right) = +1,$$

où le produit Π s'étend à tous les nombres premiers rationnels.

Démonstration. — Soient p et q deux entiers rationnels distincts impairs et tous deux premiers; les règles (a''), (b'), (b'') du paragraphe 64 et le théorème 101 nous permettent d'écrire :

$$\left(\frac{-1, 2}{2}\right) = +1, \quad \left(\frac{-1, p}{2}\right)\left(\frac{-1, p}{p}\right) = +1,$$

$$\left(\frac{2, 2}{2}\right) = +1, \quad \left(\frac{2, p}{2}\right)\left(\frac{2, p}{p}\right) = +1,$$

$$\left(\frac{p, p}{2}\right)\left(\frac{p, p}{p}\right) = +1, \quad \left(\frac{p, q}{2}\right)\left(\frac{p, q}{p}\right)\left(\frac{p, q}{q}\right) = +1;$$

et grâce à la règle (a') du paragraphe 64, le lemme 14 subsiste pour le cas où les nombres n et m égalent ± 1 ou ne contiennent qu'un nombre premier. Les formules (e''') et (e'''') montrent que le lemme 14 est général.

De $\left(\frac{-1,\ -1}{2}\right) = -1$, il résulte que si n et m sont tous deux négatifs, le produit $\prod\limits_{(w)}$ est égal à $+1$.

On peut exprimer plus simplement la proposition contenue dans le lemme 14 et celle que nous venons d'énoncer en employant le nouveau symbole $\left(\frac{n,\ m}{-1}\right) = \pm 1$, en lui donnant la valeur $+1$, si l'un des nombres n ou m est négatif, et la valeur -1 lorsqu'ils le sont tous les deux.

§ 70. — Démonstration des rapports entre l'ensemble des caractères d'un genre énoncés dans le théorème fondamental 100.

Appliquons le lemme 14. Soit $\mathfrak{A}$ une classe d'idéaux du corps $k(\sqrt{m})$, et soit $\mathfrak{a}$ un idéal de cette classe premier avec 2 et avec d, et soit $\overline{n} = \pm n(\mathfrak{a})$ la norme de l'idéal $\mathfrak{a}$ pourvue du signe prévu au paragraphe 65; le produit de tous les caractères de la classe $\mathfrak{A}$ est donné par

$$\left(\frac{\overline{n},\ m}{l_1}\right) \cdots \cdots \left(\frac{\overline{n},\ m}{l_t}\right).$$

Comme $n(\mathfrak{a})$ est la norme d'un idéal, tout nombre premier rationnel p contenu dans $\overline{n}$ se décompose dans le corps $k(\sqrt{m})$; et, par suite, d'après le théorème 96, m est reste quadratique de tout pareil nombre.

Du lemme 14, et en tenant compte des formules (e'''), (a'), (a'') du théorème 98, on a

$$\prod_{(w)} \left(\frac{\overline{n},\ m}{w}\right) = +1,$$

lorsque w prend les valeurs des nombres premiers impairs contenus dans d, ainsi que la valeur 2.

Si donc le discriminant d du corps $k(\sqrt{m})$ contient le nombre premier 2, il est démontré déjà que pour toute classe de $k(\sqrt{m})$ le produit de tous les caractères $= +1$.

Par contre, si 2 n'est pas contenu dans d, comme $m \equiv 1$ suivant 4, on a $\left(\frac{\overline{n},\ m}{2}\right) = +1$, et le théorème est aussi démontré dans ce cas.

Ayant démontré que le produit des caractères est égal à $+1$, nous reconnaissons de suite que le nombre des genres dans le corps quadratique $k(\sqrt{m})$ est au plus égal à la moitié de tous les systèmes de caractères imaginables, c'est-à-dire au plus égal à 2^{r-1}.

CHAPITRE XVIII.

L'existence des genres dans le corps quadratique.

§ 71. — Le théorème sur les normes des nombres d'un corps quadratique.

Il reste à faire voir que la seconde partie du théorème 100 est vraie, c'est-à-dire à démontrer que la condition que nous avons reconnue nécessaire pour qu'un système de r unités ± 1 forme le système de caractères d'un genre dans $k(\sqrt{m})$ est aussi suffisante. On peut y arriver par deux voies bien distinctes : la première est de nature purement arithmétique, la seconde a des moyens transcendants. La première démonstration résulte des raisonnements suivants :

Théorème 102. — Si n, m sont deux entiers rationnels, m n'étant pas un carré parfait, qui remplissent pour tout nombre premier w la condition

$$\left(\frac{n,\, m}{w}\right) = +1,$$

le nombre n est toujours la norme d'un nombre entier ou fractionnaire α du corps $k(\sqrt{m})$.

Démonstration. — La condition $\prod_w \left(\frac{n,\, m}{w}\right)$ exige, comme il résulte de la remarque faite à la fin du paragraphe 69, que l'un des nombres n ou m au moins soit positif. Nous pouvons admettre que n et m ne renferment pas de facteur rationnel au carré. Soit alors p un facteur premier de n qui divise aussi le discriminant d du corps $k(\sqrt{m})$: p est la norme d'un idéal de $k(\sqrt{m})$. De plus, si p est un nombre premier impair qui divise n et m ou m, comme $\left(\frac{n,\, m}{p}\right) = \left(\frac{m}{p}\right) = +1$, p est aussi la norme d'un idéal de $k(\sqrt{m})$. Enfin, si 2 divise n et ne divise pas le discriminant du corps $k(\sqrt{m})$, comme $\left(\frac{n,\, m}{2}\right) = \left(\frac{2,\, m}{2}\right) = (-1)^{\frac{m^2-1}{8}} = +1$, 2 est encore la norme d'un idéal de $k(\sqrt{m})$, et, par suite, $k(\sqrt{m})$ contient certainement un idéal $\mathfrak{j}$, tel que $n = n(\mathfrak{j})$. Choisissons dès lors dans la classe d'idéaux déterminée par $\mathfrak{j}$ un

idéal $\mathfrak{j}'$, dont la norme $n(\mathfrak{j}') \leqslant |\sqrt{d}|$ où d est le discriminant du corps $k(\sqrt{m})$. Ceci, d'après le théorème 50, est toujours possible. Nous poserons $\mathfrak{j}' = \varkappa\mathfrak{j}$ et $n' = n.n(\varkappa)$, où $\varkappa$ est un nombre entier ou fractionnaire de $k(\sqrt{m})$; on aura $n' = \pm n(\mathfrak{j}')$ avec le signe $+$ ou le signe $-$ suivant que $n(\varkappa)$ est positif ou négatif. Le nombre entier rationnel n' est donc en particulier sûrement positif lorsque m est négatif. Comme d a pour valeur m ou $4m$, on a $|n'| \leqslant 2|\sqrt{m}|$, et il en résulte $|n'| < |m|$ dès que $2|\sqrt{m}| < |m|$, c'est-à-dire $|m| > 4$. D'autre part, comme $n' = n.n(\varkappa)$, on a $\left(\frac{n,\, m}{w}\right) = \left(\frac{n',\, m}{w}\right) = +1$, et, par suite, à cause de la formule (e'') du théorème 98,

$$\left(\frac{m,\, n'}{w}\right) = +1$$

pour tout nombre premier w.

Admettons que le théorème 102, que nous voulons démontrer, soit vrai pour tout corps $k(\sqrt{m})$ pour lequel le nombre m', qu'il soit positif ou négatif, satisfait à $|m'| < |m|$. Le nombre n' que nous venons de trouver satisfait à $|n'| < |m|$ et n'est pas un carré, et comme on a de plus $\left(\frac{m,\, n'}{w}\right) = +1$ pour tout nombre premier w, il faut, grâce à notre hypothèse, que le nombre m soit la norme d'un nombre $\varkappa'$ dans le corps $k(\sqrt{n'})$, c'est-à-dire qu'il existe deux nombres entiers ou fractionnaires rationnels tels que

$$m = a^2 - n'b^2;$$

d'autre part, si n' est un carré, la possibibilité de cette égalité est évidente. Comme il faut que b soit $\neq 0$, on voit que $n' = \left(\frac{a}{b}\right)^2 - m\left(\frac{1}{b}\right)^2 = n(\lambda)$, c'est-à-dire que n' est la norme d'un nombre λ dans le corps $k(\sqrt{m})$. En rapprochant ce fait de $n' = n.n(\varkappa)$, on voit que $n = n(\varkappa)$, où $\varkappa = \frac{\lambda}{\varkappa}$ est encore un nombre de $k(\sqrt{m})$.

La démonstration complète du théorème 102 sera accomplie dès que nous aurons montré que le théorème est vrai pour $|m| \leqslant 4$ avec $|n| \leqslant |\sqrt{d}|$. En restreignant ainsi les nombres n et m, les conditions du théorème 102 ne sont remplies que dans huit cas.

Les égalités

$$1 = n(\sqrt{-1}), \qquad -2 = n(\sqrt{2}),$$
$$2 = n(1 + \sqrt{-1}), \qquad 2 = n(\sqrt{-2}),$$
$$2 = n(2 + \sqrt{2}), \qquad 2 = n(1 + \sqrt{3}),$$
$$-1 = n(1 + \sqrt{2}), \qquad -3 = n(\sqrt{3})$$

montrent que dans ces huit cas le théorème 102 est vrai.

On reconnaît que le théorème 102 est encore vrai si on en modifie l'énoncé en exigeant que la condition $\left(\frac{n,\, m}{w}\right) = +1$ ne soit remplie que pour tous les nombres premiers impairs w; mais il faut alors ajouter cette condition que l'un des nombres n et m au moins est négatif. [Lagrange[1], Legendre[1], Gauss[1].] Et, en effet, d'après le lemme 14, l'égalité $\left(\frac{n,\, m}{2}\right) = +1$ est alors satisfaite d'elle-même.

§ 72. — Les classes du genre principal.

A la fin du paragraphe 66 nous avons montré que le carré d'une classe d'idéaux appartient toujours au genre principal. Le théorème 102 du paragraphe 71 nous permet de montrer la réciproque.

Théorème 103. — Dans un corps quadratique, toute classe du genre principal est le carré d'une classe. [Gauss[1].]

Démonstration. — Soit H une classe du genre principal du corps $k(\sqrt{m})$ et $\mathfrak{h}$ un idéal de cette classe première avec le d du corps $k(\sqrt{m})$, soit $\bar{n}$ la norme de l'idéal $\mathfrak{h}$ précédée du signe prévu au paragraphe 65. Ce nombre $\bar{n}$ remplit alors, quel que soit le nombre premier w, la condition $\left(\frac{\bar{n},\, m}{w}\right) = +1$, et par suite on a $\bar{n} = n(\alpha)$, où α est un nombre entier ou fractionnaire du corps $k(\sqrt{m})$. Posons donc $\frac{\mathfrak{h}}{\alpha} = \frac{\mathfrak{j}}{\mathfrak{j}'}$, $\mathfrak{j}$ et $\mathfrak{j}'$ étant des idéaux premiers entre eux; il en résulte que $\frac{\mathfrak{j}\, s\mathfrak{j}}{\mathfrak{j}'\, s\mathfrak{j}'} = 1$ et, par suite, $\mathfrak{j}' = s\mathfrak{j}$. Comme $\mathfrak{j}\, s\mathfrak{j} \sim 1$, il en résulte que $\mathfrak{h} \sim \mathfrak{j}^2$.

Cette propriété caractéristique des idéaux du genre principal a un rapport étroit avec une autre propriété également caractéristique de ces idéaux et qui est exprimée par le théorème suivant :

Théorème 104. — Soient ω_1, ω_2 deux nombres de base du corps quadratique k et ι_1, ι_2 deux nombres de base d'un idéal $\mathfrak{h}$ appartenant au genre principal de k, et enfin soit N un nombre entier rationnel quelconque donné; on peut toujours trouver quatre nombres rationnels r_{11}, r_{12}, r_{21}, r_{22} dont les dénominateurs sont premiers avec N, dont le déterminant $r_{11}r_{22} - r_{21}r_{12} = \pm 1$, et tels que

$$\frac{\iota_1}{\iota_2} = \frac{r_{11}\omega_1 + r_{12}\omega_2}{r_{21}\omega_1 + r_{22}\omega_2}.$$

Démonstration. — Déterminons un idéal $\mathfrak{h}'$ équivalent à $\mathfrak{h}$; $\mathfrak{h}' = \rho\mathfrak{h}$ premier avec Nd.

Ainsi que nous l'avons déjà utilisé dans la démonstration du théorème 103, $\bar{n} = \pm n(\mathfrak{h}')$ est égal à la norme d'un nombre α entier ou fractionnaire du corps k, si l'on choisit le signe + ou le signe — d'après les conventions du paragraphe 65.

L'idéal $\alpha\mathfrak{h}' = \alpha\beta\mathfrak{h}$ admet les nombres de base

$$\alpha\beta\gamma_{11} = a_{11}\omega_1 + a_{12}\omega_2,$$
$$\alpha\beta\gamma_{12} = a_{21}\omega_1 + a_{22}\omega_2,$$

où $a_{11}, a_{12}, a_{21}, a_{22}$ sont des entiers rationnels. Comme $n(\alpha\mathfrak{h}') = n^2$, le déterminant $a_{11}a_{22} - a_{12}a_{21} = \pm n^2$, et par suite les quatre nombres

$$r_{11} = \frac{a_{11}}{n}, \quad r_{12} = \frac{a_{12}}{n}, \quad r_{21} = \frac{a_{21}}{n}, \quad r_{22} = \frac{a_{22}}{n}$$

ont les propriétés indiquées dans l'énoncé.

§ 73. — Les idéaux ambiges.

Nous dirons qu'un idéal $\mathfrak{a}$ du corps k est un *idéal ambige* si l'opération $s = (\sqrt{m} : -\sqrt{m})$ le laisse inaltéré et s'il ne contient pas d'autre facteur entier rationnel que ± 1 (voir § 57). On a le

Théorème 105. — Les t idéaux premiers $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_t$ distincts contenus dans le discriminant d du corps k sont des idéaux ambiges premiers du corps k, et il n'y en a pas d'autres. Les 2^t idéaux $1, \mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2, \ldots, \mathfrak{l}_1\mathfrak{l}_2\ldots\mathfrak{l}_t$ forment l'ensemble de tous les idéaux ambiges du corps k.

Démonstration. — Que les idéaux premiers $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ sont ambiges et qu'il n'y en a pas d'autres, cela résulte du théorème 90. Soit maintenant $\mathfrak{a} = \mathfrak{p}.\mathfrak{q}\ldots\mathfrak{r}$ un idéal ambige quelconque décomposé en idéaux premiers; comme $\mathfrak{a} = s\mathfrak{a}$, il faut que les idéaux conjugués à $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}, s\mathfrak{p}, s\mathfrak{q}, \ldots, s\mathfrak{r}$, abstraction faite de leur ordre, soient égaux à $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$. Si on avait, par exemple, $s\mathfrak{p} = \mathfrak{q}$, $\mathfrak{a}$ contiendrait le facteur $\mathfrak{p}s\mathfrak{p}$, qui est un entier rationnel; comme ceci est contraire à la définition d'un idéal ambige, il faut que $\mathfrak{p} = s\mathfrak{p}$, $\mathfrak{q} = s\mathfrak{q}, \ldots$, c'est-à-dire que tous les idéaux soient ambiges. Comme les carrés des idéaux $\mathfrak{l}, \ldots, \mathfrak{l}_t$ sont des entiers rationnels, nous en conclurons que $\mathfrak{p}, \mathfrak{q}, \ldots, \mathfrak{r}$ sont nécessairement distincts, et la dernière partie du théorème 105 est démontrée.

§ 74. — Les classes ambiges d'idéaux.

Soit $\mathfrak{a}$ un idéal de la classe A; nous désignerons par sA la classe à laquelle appartient $s\mathfrak{a}$. Et, en particulier, si $A = sA$, la classe d'idéaux A est dite une *classe ambige d'idéaux*. Comme le produit $\mathfrak{a}s\mathfrak{a} \sim 1$, $A.sA = 1$; et par suite, le carré de toute classe ambige est égal à la classe principale 1. Réciproquement, lorsque le carré d'une classe A égale 1, $A = \frac{1}{A} = sA$, et par suite la classe A est ambige.

§ 75. Les classes ambiges d'idéaux déterminées par les idéaux ambiges.

Il s'agit maintenant d'établir les classes ambiges de k. Comme tout idéal ambige $\mathfrak{a}$ détermine une classe ambige en vertu de sa propriété $\mathfrak{a} = s\mathfrak{a}$, il nous faut d'abord rechercher combien de classes ambiges distinctes résultent des 2^t idéaux ambiges. Nous dirons que plusieurs classes d'idéaux sont *classes d'idéaux indépendantes* lorsqu'aucune d'elles n'est égale à la classe 1 et lorsqu'elle n'est pas non plus égale à un produit de puissances des autres classes. Nous énoncerons alors le

Théorème 106. — Les t idéaux premiers ambiges déterminent toujours $t-1$ classes ambiges indépendantes dans le cas d'un corps imaginaire; dans le cas d'un corps réel, elles déterminent $t-2$ ou $t-1$ classes indépendantes, suivant que la norme de l'unité fondamentale ε du corps $n(\ ) = +1$ ou -1. L'ensemble des 2^t idéaux ambiges détermine, dans le cas d'un corps imaginaire 2^{t-1} et dans le cas d'un corps réel 2^{t-2} ou 2^{t-1} classes indépendantes, la distinction entre 2^{t-2} ou 2^{t-1} se faisant par le signe de $n(\varepsilon)$.

Démonstration. — Le produit de tous les idéaux premiers facteurs de m est égal à $\sqrt{m}$; il est donc un idéal principal de k. Soit d'abord m négatif, mais différent de -1 et de -3, et soit (α) un idéal principal ambige de k; on a nécessairement $\alpha^{1-s} = (-1)^e$, car α^{1-s} est une unité, e ne pouvant être égal qu'à 0 ou à 1. Il en résulte que

$$\{\alpha(\sqrt{m})^e\}^{1-s} = 1 \quad \text{ou} \quad \alpha(\sqrt{m})^e = s\{\alpha(\sqrt{m})^e\},$$

c'est-à-dire que $\alpha(\sqrt{m})^e$ est un entier rationnel. Ce qui démontre que dans un corps imaginaire, $k(\sqrt{-1})$ et $k(\sqrt{-3})$ exceptés, il ne peut y avoir d'autre idéal principal ambige que 1 et $\sqrt{m}$. Les deux exceptions, traitées en particulier, donnent immédiatement le résultat énoncé au théorème 106.

Soit un corps réel, pour lequel $n(\varepsilon) = +1$; d'après le théorème 90, $\varepsilon = \alpha^{1-s}$, où α est un nombre de k que nous avons le droit de supposer dégagé de tout facteur rationnel différent de ± 1. Comme $\alpha = \varepsilon . s\alpha$, (α) est un idéal principal ambige. Cet idéal principal (α) est distinct de 1 et de $\sqrt{m}$, car si l'on avait $\alpha = \pm\varepsilon^f$ ou $\pm\varepsilon^f\sqrt{m}$, où f est un entier rationnel, on aurait

$$\alpha^{1-s} = (-1)^e\varepsilon^{f(1-s)} = (-1)^e\varepsilon^{2f} \quad (e = 0 \text{ ou } 1),$$

mais ce nombre est toujours différent de ε. Si, d'autre part, α' est un idéal principal ambige quelconque du corps k, on a nécessairement $\alpha'^{1-s} = (-1)^e\varepsilon^f$, où e et f sont des entiers rationnels. Posons $\alpha'' = \dfrac{\alpha'}{(\sqrt{m})^e\alpha^f}$; on voit que $\alpha''^{1-s} = 1$, c'est à dire que

α'' est un nombre rationnel, et par suite, outre 1, $\sqrt{m}$ et α, il ne peut y avoir qu'un idéal principal ambige obtenu en débarrassant le produit $\sqrt{m}.\alpha$ de tout facteur rationnel différent de ± 1.

D'autre part, si $n(\varepsilon) = -1$, il n'y a pas dans k d'idéal principal ambige différent de 1 et de $\sqrt{m}$, car, soit α un idéal ambige quelconque de k, on aurait nécessairement

$$\alpha^{1-S} = (-1)^{e}\varepsilon^{f}$$

avec e et f entiers rationnels, et comme $n(\alpha^{1-S}) = +1$, $(n(\varepsilon))^{f} = +1$, c'est-à-dire que f est pair. Posons

$$\alpha' = \frac{\alpha}{\varepsilon^{\frac{f}{2}}(\sqrt{m})^{e+\frac{f}{2}}},$$

nous trouvons $\alpha'^{1-S} = +1$, c'est-à-dire que α' est un nombre rationnel.

Nous exprimerons donc un des t idéaux premiers ambiges de k approprié au moyen de $\sqrt{m}$ et des $t-1$ autres idéaux premiers ambiges, et lorsque le corps est réel et que $n(\varepsilon) = +1$, nous choisirons parmi ces $t-1$ idéaux premiers ambiges un idéal approprié que nous exprimerons au moyen de α et des $t-2$ autres. Ceci nous montre que la deuxième partie du théorème 106 est exacte.

§ 76. — Les classes ambiges d'idéaux qui ne contiennent pas d'idéal ambige.

Théorème 107. — La condition nécessaire et suffisante pour qu'un corps quadratique k contienne une classe ambige qui ne contienne pas elle-même d'idéal ambige est que le système de caractères de -1 soit composé d'unités toutes positives et que la norme de l'unité fondamentale $n(\varepsilon) = +1$. Lorsque ces conditions sont remplies, les classes ayant cette propriété s'obtiennent en multipliant l'une quelconque d'entre elles successivement par chacune des classes provenant des idéaux ambiges.

Démonstration. — Lorsque le corps k est réel et que le système des caractères de -1 n'est composé que d'unités positives, il y a toujours dans k, d'après le théorème 102, un uombre entier ou fractionnaire α dont la norme égale -1. Si, de plus, la norme de l'unité fondamentale $n(\varepsilon) = +1$, ce nombre α est nécessairement fractionnaire. Posons $\alpha = \frac{\mathfrak{j}}{\mathfrak{j}'}$, où $\mathfrak{j}$ et $\mathfrak{j}'$ sont des idéaux premiers entre eux; il en résulte que $\frac{\mathfrak{j}s\mathfrak{j}}{\mathfrak{j}'s\mathfrak{j}'} = 1$, et par suite $\mathfrak{j}' = s\mathfrak{j}$; par suite, $\mathfrak{j} \sim s\mathfrak{j}$ et $\mathfrak{j}$ détermine une classe ambige. Cette classe ambige ne contient pas d'idéal ambige, car si un idéal de cette classe $\mathfrak{a} = \mathfrak{j}\beta$, où β est un nombre de k entier ou fractionnaire, était ambige, on en conclurait que $\mathfrak{a}^{1-S} = \alpha\beta^{1-S}$, et par suite $\alpha\beta^{1-S}$ serait une unité, par exemple $= (-1)^{e}\varepsilon^{f}$, et par suite $n(\alpha) = +1$, ce qui est contraire à la façon dont α a été obtenu. Ceci nous prouve que la classe $\mathfrak{j}$ ne contient pas d'idéal ambige.

Soit maintenant A une classe ambige quelconque donnée et $\mathfrak{j}$ un de ses idéaux, $\mathfrak{j}^{1-S}$ est égal à un nombre entier ou fractionnaire α du corps k et, de plus, $n(\alpha) = +1$ ou -1. Le premier cas est le seul possible, lorsque le corps est imaginaire ou lorsque le corps k est réel et que l'un au moins des caractères $\left(\frac{-1,\, m}{w}\right)$ est égal à -1. Comme $n(\alpha) = +1$, il résulte du théorème 90 que $\frac{1}{\alpha} = \beta^{1-S}$, β étant un nombre entier de k, et alors $(\mathfrak{j}\beta)^{1-S} = 1$, c'est-à-dire que $\mathfrak{j}\beta$ est le produit d'un idéal ambige par un nombre rationnel et la classe A contient un idéal ambige. D'autre part, si $n(\alpha) = -1$ avec $n(\varepsilon) = -1$, $n(\varepsilon\alpha) = +1$, et nous démontrerons comme précédemment que la classe A contient un idéal ambige. Ceci nous montre que toute classe ambige contient un idéal ambige dans le cas où le corps est imaginaire ou bien dans le cas où le corps est réel et que l'un des caractères de -1 égale -1, ou encore que $n(\varepsilon) = -1$.

Admettons maintenant que, dans le cas où aucune de ces circonstances ne se produit, il y ait dans k plusieurs classes ambiges d'idéaux qui ne contiennent pas d'idéal ambige, et prenons dans l'une d'elles un idéal $\mathfrak{j}$, dans une autre un idéal $\mathfrak{j}'$; les développements qui précèdent montrent que les normes des deux nombres $\alpha = \mathfrak{j}^{1-S}$, $\alpha' = \mathfrak{j}'^{1-S}$ sont égales toutes deux à -1, et par suite $n\left(\frac{\alpha'}{\alpha}\right) = +1$. Le théorème 90 nous permet de mettre $\frac{\alpha}{\alpha'} = \beta^{1-S}$, β un nombre convenablement choisi de k. Posons $\frac{\mathfrak{j}'\beta}{\mathfrak{j}} = b\mathfrak{a}$, où b est rationnel et $\mathfrak{a}$ un idéal sans facteur rationnel $\neq \pm 1$, $\left(\frac{\mathfrak{j}'\beta}{\mathfrak{j}}\right)^{1-S} = 1$ entraîne $\mathfrak{a} = S\mathfrak{a}$, c'est-à-dire que $\mathfrak{a}$ est un idéal ambige, et on a $\mathfrak{j}' = \mathfrak{a}\mathfrak{j}$. Ce qui démontre la dernière partie du théorème 107.

§ 77. — Le nombre de toutes les classes ambiges.

Les théorèmes 106 et 107 permettent d'énumérer toutes les classes ambiges.

Théorème 108. — Dans tous les cas, le corps k contient exactement $r-1$ classes ambiges indépendantes, r étant le nombre des caractères qui détermine le genre d'une classe. Le nombre total des classes ambiges distinctes est par suite 2^{r-1}.

Démonstration. — Soit encore t le nombre des entiers premiers rationnels contenus dans le discriminant d du corps k. Considérons d'abord le cas où k est un corps imaginaire. Il résulte des théorèmes 106 et 107 qu'il y a exactement 2^{t-1} classes ambiges dans k; elles résultent toutes d'idéaux ambiges. Supposons le corps k réel : si le système des caractères de -1 dans k ne contient que des unités positives, il y a exactement 2^{t-1} classes ambiges dans k; ces 2^{t-1} proviennent toutes d'idéaux ambiges

ou la moitié d'entre elles proviennent d'idéaux ambiges suivant que $n(\varepsilon) = -1$ ou $n(\varepsilon) = +1$. Toutefois, si -1 a au moins un caractère négatif, $n(\varepsilon) = +1$, et les théorèmes 106 et 107 nous affirment qu'il n'y a alors que 2^{t-2} classes ambiges dans k, provenant toutes d'idéaux ambiges. Mais le nombre des caractères $= t - 1$ lorsque le corps est réel et que le nombre -1 a au moins un caractère négatif; on a $r = t$ dans tous les autres cas. Le théorème 108 est démontré.

§ 78. — La démonstration arithmétique de l'existence des genres.

Les résultats acquis nous permettent d'évaluer le nombre des genres et de répondre à la question posée au théorème 100; car il nous est facile de démontrer que ce nombre est égal à 2^{r-1} et, par suite, que tous les systèmes de caractères qui satisfont aux conditions du théorème 100 sont représentés parmi les genres. Nous désignerons par g le nombre des genres et par f le nombre des classes du genre principal. D'après le paragraphe 66, tous les genres renferment le même nombre de classes, par suite le nombre des classes $h = gf$. Désignons par $H_1, \ldots, H_f$ les f classes du genre principal; le théorème 103 nous apprend que nous pouvons écrire $H_1 = K_1^2, \ldots, H_f = K_f^2$, où $K_1, \ldots, K_f$ représentent f certaines classes du corps.

Soit alors C une classe quelconque du corps; comme C^2 appartient au genre principal, $C^2 = K_a^2$, où K_a représente une classe bien déterminée parmi les f classes $K_1, \ldots, K_f$ que nous venons de définir. Alors la classe $\frac{C}{K_a}$, c'est-à-dire la classe A parfaitement déterminée pour laquelle $C = AK_a$, est une classe ambige et par suite l'expression AK, où A représente successivement toutes les classes ambiges et où K prend toutes les valeurs $K_1, \ldots, K_f$, fournit toutes les classes du corps et ne donne chacune d'elles qu'une fois. Mais d'après le théorème 108, le nombre des classes ambiges est 2^{r-1}; par suite $h = 2^{r-1}f$, et comme $h = gf$, on voit que $g = 2^{r-1}$. Le théorème fondamental 100 est complètement démontré. [Gauss[1].]

§ 79. — La représentation transcendante du nombre des classes; elle permet d'établir que la limite d'un certain produit infini est positive.

La deuxième démonstration de l'existence des 2^{r-1} genres s'appuie sur des considérations transcendantes.

Théorème 109. — Le nombre h des classes d'idéaux du corps k de discriminant d est déterminé par la formule

$$\varkappa h = \lim_{s=1} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}};$$

le produit du second membre s'étend à tous les nombres premiers p rationnels et le symbole $\left(\frac{d}{p}\right)$ a le sens fixé au paragraphe 61. Le facteur $\varkappa$, suivant que k est imaginaire ou réel, c'est-à-dire suivant que d est négatif ou positif, a la valeur

$$\varkappa = \frac{2\pi}{w|\sqrt{d}|} \quad \text{ou} \quad \varkappa = \frac{2\log\varepsilon}{|\sqrt{d}|};$$

w a la valeur 6 pour $d = -3$, pour $d = -4$ la valeur 4; il est égal à 2 pour toute autre valeur négative de d; d'autre part, pour tout corps réel ε sera celle de ses quatre unités fondamentales, qui est > 1, et $\log \varepsilon$ sera la partie réelle du logarithme de cette unité fondamentale ε. [Dirichlet[8, 9].]

Démonstration. — D'après le paragraphe 27, on a, tant que s est réel et > 1 :

$$\zeta(s) = \sum_{(\mathfrak{j})} \frac{1}{n(\mathfrak{j})^s} = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}},$$

le produit s'étendant à tous les idéaux premiers du corps k. Ordonnons ce produit d'après les nombres premiers rationnels p d'où proviennent ces idéaux premiers $\mathfrak{p}$; on voit, d'après le théorème 97, qu'à tout nombre premier rationnel p correspond dans ce produit le facteur

$$\frac{1}{(1 - p^{-s})^2} \quad \text{ou} \quad \frac{1}{1 - p^{-2s}} \quad \text{ou} \quad \frac{1}{1 - p^{-s}},$$

suivant que $\left(\frac{d}{p}\right) = +1, = -1, = 0$. Nous écrirons ces trois expressions sous une forme qui leur est commune

$$\frac{1}{1 - p^{-s}} \cdot \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}},$$

et nous obtenons

$$\zeta(s) = \prod_{(p)} \frac{1}{1 - p^{-s}} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}},$$

où les deux produits du second membre s'étendent à tous les nombres premiers rationnels p. En vertu de

$$\underset{s=1}{\mathrm{L}} \left\{ (s-1) \prod_{(p)} \frac{1}{1 - p^{-s}} \right\} = \underset{s=1}{\mathrm{L}} \left\{ (s-1) \sum_{(n)} \frac{1}{n^s} \right\} = 1,$$

où n prend toutes les valeurs entières rationnelles,

$$\underset{s=1}{\mathrm{L}} \left\{ (s-1)\zeta(s) \right\} = \underset{s=1}{\mathrm{L}} \prod_{(p)} \frac{1}{1 - \left(\frac{d}{p}\right) p^{-s}}.$$

Notre théorème 109 va résulter du théorème 56, si nous évaluons $\varkappa$ d'après le paragraphe 25. Pour trouver w, il faut remarquer que le corps $k(\sqrt{-3})$ contient six racines de l'unité ± 1, $\pm \frac{1 \pm \sqrt{-3}}{2}$ et que le corps $k(\sqrt{-1})$ contient les quatre racines de l'unité ± 1, $\pm i$; par contre, tout autre corps imaginaire k ne contient que les deux racines de l'unité ± 1. (Comparez § 62.)

La conséquence la plus importante que nous en tirerons est le

THÉORÈME 110. — Soit a un nombre entier rationnel quelconque positif ou négatif, non carré parfait; la limite de

$$\underset{s=1}{\mathrm{L}} \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

est toujours une grandeur finie différente de o. [Dirichlet[8, 9].]

Démonstration. — Soit $a = b^2 m$, b^2 étant le plus grand carré contenu dans a; soit, de plus, d le discriminant du corps déterminé par $\sqrt{a}$. Pour tout nombre premier impair p qui ne divise pas b, on a $\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right)$ les deux produits infinis

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} \quad \text{et} \quad \prod_{(p)} \frac{1}{1-\left(\frac{a}{p}\right)p^{-s}}$$

ne peuvent différer que d'un nombre fini de facteurs. Le premier produit restant fini pour $s = 1$, d'après le théorème 109, il s'ensuit que le second tend vers une limite finie.

§ 80. — Il y a une infinité de nombres premiers rationnels par rapport auxquels les caractères de restes quadratiques des nombres donnés sont donnés.

Le théorème 110 va nous permettre de démontrer les propositions suivantes : [Dirichlet[9], Kronecker[10].]

THÉORÈME 111. — Soient $a_1, a_2, \ldots, a_t$, t nombres entiers rationnels quelconques positifs ou négatifs, mais tels qu'aucun des $2^t - 1$ nombres $a_1, a_2, \ldots, a_t$; $a_1 a_2, \ldots, a_{t-1} a_t$; $\ldots$, $a_1 a_2 \ldots a_t$ ne soit un carré, et désignons par $c_1, c_2, \ldots, c_t$, t unités quelconques $+1$ ou -1, il y a une infinité de nombres premiers rationnels p, tels que

$$\left(\frac{a_1}{p}\right) = c_1, \quad \left(\frac{a_2}{p}\right) = c_2, \quad \ldots, \quad \left(\frac{a_t}{p}\right) = c_t.$$

Démonstration. — Tant que $s > 1$,

$$\log \sum_{(n)} \frac{1}{n^s} = \sum_{(p)} \log \frac{1}{1 - p^{-s}} = \sum_{(p)} \frac{1}{p^s} + \mathrm{S},$$

$$\mathrm{S} = \frac{1}{2} \sum_{(p)} \frac{1}{p^{2s}} + \frac{1}{3} \sum_{(p)} \frac{1}{p^{3s}} + \ldots .$$

L'expression S, on l'a montré au paragraphe 50, reste finie pour $s = 1$; il en résulte que la somme étendue à tous les nombres premiers rationnels p

$$(26) \qquad \sum_{(p)} \frac{1}{p^s}$$

croît au delà de toute limite lorsque s tend vers l'unité. Soit, de plus, a un nombre entier rationnel quelconque; on a pour $s > 1$

$$\log \prod_{(p)} \frac{1}{1 - \left(\dfrac{a}{p}\right) p^{-s}} = \sum_{(p)} \left(\frac{a}{p}\right) \frac{1}{p^s} + \mathrm{S}_a,$$

$$\mathrm{S}_a = \frac{1}{2} \sum_{(p)} \left(\frac{a}{p}\right)^2 \frac{1}{p^{2s}} + \frac{1}{3} \sum_{(p)} \left(\frac{a}{p}\right)^3 \frac{1}{p^{3s}} + \ldots .$$

Lorsque a n'est pas carré parfait, nous savons (théorème 110) que $\log \prod_{(p)} \frac{1}{1 - \left(\frac{a}{p}\right) p^{-s}}$ est fini pour $s = 1$, et, comme on peut en dire autant de S_a, il en résulte que la somme

$$(27) \qquad \sum_{(p)} \left(\frac{a}{p}\right) \frac{1}{p^s}$$

tend vers une limite finie pour $s = 1$. Remplaçons dans (27)

$$a = a_1^{u_1} a_2^{u_2}, \ldots, a_t^{u_t},$$

et donnons à chacun des t exposants $a_1, a_2, \ldots, a_t$ la valeur 0 ou 1, en exceptant toutefois le système de valeurs

$$u_1 = 0, \quad u_2 = 0, \quad \ldots, \quad u_t = 0.$$

Multiplions ensuite chacune des sommes déduites ainsi de (27) par le facteur correspondant $c_1^{u_1} c_2^{u_2} c_t^{u_t}$, et additionnant les $2^t - 1$ expressions à (26), il nous vient

$$(28) \qquad \sum_{(p)} \left(1 + c_1 \left(\frac{a_1}{p}\right)\right) \left(1 + c_2 \left(\frac{a_2}{p}\right)\right) \cdots \left(1 + c_t \left(\frac{a_t}{p}\right)\right) \frac{1}{p^s}.$$

Cette somme, tout comme la somme 26, croîtra indéfiniment quand s tend vers 1. Faisant abstraction des nombres premiers p contenus dans $a_1, a_2, \ldots, a_t$, et qui sont en nombre fini, la somme (28) égale $2^t \prod_{(p')} \frac{1}{p'^s}$, où p' ne prend que les valeurs des nombres premiers p qui remplissent toutes les conditions de l'énoncé du théorème 111. Et comme cette somme croît elle aussi au delà de toute limite, il faut que les nombres premiers p' existent en nombre infini. Le théorème 111 est démontré.

§ 81. — L'existence d'une infinité d'idéaux premiers de caractères donnés dans un corps quadratique.

THÉORÈME 112. — Soient

$$\chi_1 = \left(\frac{\pm n(\mathfrak{j}),\, m}{l_1}\right), \quad \ldots, \quad \chi_r(\mathfrak{j}) = \left(\frac{\pm n(\mathfrak{j}),\, m}{l_r}\right)$$

les r caractères qui déterminent le genre d'un idéal $\mathfrak{j}$ de k, et soient $c_1, \ldots, c_r$, r unités quelconques $= \pm 1$ satisfaisant à la condition $c_1 \ldots c_r = +1$; il y a une infinité d'idéaux premiers $\mathfrak{p}$ du corps k pour lesquels

$$\chi_1(\mathfrak{p}) = c_1, \quad \ldots, \quad \chi_r(\mathfrak{p}) = c_r.$$

Démonstration. — Supposons que le discriminant du corps contienne les t nombres premiers rationnels $l_1, \ldots, l_t$; $t = r$ ou $= r+1$, dans ce dernier cas, soit $\left(\frac{-1,\, m}{l_t}\right) = -1$, et la condition $\left(\frac{\pm n(\mathfrak{j}),\, m}{l_t}\right) = +1$ servira à déterminer le signe devant $n(\mathfrak{j})$. Nous écrirons dans ce cas $c_t = c_{r+1} = +1$. Nous démontrerons d'abord qu'il y a une infinité de nombres premiers rationnels p pour lesquels

$$\left(\frac{p,\, m}{l_1}\right) = c_1, \quad \ldots, \quad \left(\frac{p,\, m}{l_t}\right) = c_t,$$

et nous distinguerons pour cela trois cas, suivant que

$$m \equiv 1, \qquad m \equiv 3 \qquad \text{ou} \qquad m \equiv 2 \text{ suivant } 4.$$

Dans le premier cas, nous partirons de l'hypothèse

$$\left(\frac{-1}{p}\right) = +1, \quad \left(\frac{l_1}{p}\right) = c_1, \quad \ldots, \quad \left(\frac{l_t}{p}\right) = c_t.$$

Le théorème 111 nous apprend qu'il y a une infinité de nombres premiers p qui satisfont à ces conditions. Comme la première condition revient à $p \equiv 1$ suivant 4, on a pour ces nombres premiers p

$$\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i,$$

pour $i = 1, \ldots, t$.

Dans le second cas, désignons par l_s celui des nombres premiers $l_1, \ldots, l_t$, qui est égal à 2. Soit alors $c_s = -1$; nous prendrons comme point de départ l'hypothèse

$$\left(\frac{-1}{p}\right) = -1, \quad \left(\frac{l_i}{p}\right) = c_i \quad (i = 1, \ldots, s-1,\ s+1, \ldots, t).$$

et il résulte du théorème 111 qu'il existe une infinité de nombres premiers p satisfaisant à ces conditions. La première égalité nous apprend que $\left(\frac{p,\, m}{2}\right) = +1 = c_z$, et, de plus,

$$\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i,$$

pour $i = 1, \ldots, z-1, z+1, \ldots, t$.

Par contre, si $c_z = -1$, nous admettrons que

$$\left(\frac{-1}{p}\right) = -1, \quad \left(\frac{l_i}{p}\right) = (-1)^{\frac{l_i-1}{2}} c_i \quad (i=1, \ldots, z-1, z+1, \ldots, t),$$

et les nombres premiers (en nombre infini) qui remplissent ces conditions satisfont aussi à

$$\left(\frac{p,\, m}{2}\right) = -1 = c_z \quad \text{et} \quad \left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = (-1)^{\frac{l_i-1}{2}} \left(\frac{l_i}{p}\right) = c_i,$$

pour $i = 1, \ldots, z-1, z+1, \ldots, t$.

Dans le troisième cas, nous considérerons en particulier $l_z = 2$. Nous admettrons que

$$\left(\frac{-1}{p}\right) = +1, \quad \left(\frac{2}{p}\right) = c_z, \quad \left(\frac{l_i}{p}\right) = c_i \quad (i=1, \ldots, z-1, z+1, \ldots, t);$$

le théorème 111 nous montre qu'il y a une infinité de nombres premiers satisfaisant à ces conditions et pour lesquels

$$\left(\frac{p,\, m}{2}\right) = (-1)^{\frac{p^2-1}{8} + \frac{p-1}{2} \cdot \frac{m-1}{2}} = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right) = c_z,$$

et, de plus,

$$\left(\frac{p,\, m}{l_i}\right) = \left(\frac{p}{l_i}\right) = \left(\frac{l_i}{p}\right) = c_i,$$

pour $i = 1, \ldots, z-1, z+1, \ldots, t$.

Soit alors p l'un quelconque des nombres premiers rationnels p, tels que

$$\left(\frac{p,\, m}{l_1}\right) = c_1, \quad \ldots, \quad \left(\frac{p,\, m}{l_t}\right) = c_t.$$

D'après le lemme 14, on a

$$\prod_{(w)} \left(\frac{p,\, m}{w}\right) = \left(\frac{p,\, m}{p}\right)\left(\frac{p,\, m}{l_1}\right) \cdots \left(\frac{p,\, m}{l_t}\right) = +1,$$

et, par suite,

$$\left(\frac{m}{p}\right) c_1 \ldots c_t = \left(\frac{m}{p}\right) = +1,$$

c'est-à-dire que p, dans le corps k, se décompose en deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{p}'$. Chacun de ces idéaux $\mathfrak{p}$ et $\mathfrak{p}'$ répond aux conditions du théorème 112 : c'est ce que nous voulions démontrer.

§ 82. — La démonstration transcendante de l'existence des genres et des résultats énoncés du § 71 au § 77.

Le théorème 112 démontre l'existence des 2^{r-1} genres, mais il nous fait découvrir aussi un fait plus profond.

Théorème 113. — Parmi les idéaux d'un genre quelconque du corps quadratique, il y a une infinité d'idéaux premiers.

Lorsqu'on a démontré l'existence des 2^{r-1} genres par ces moyens transcendants et indépendamment des théorèmes 102, 103 et 108, il est facile d'en déduire aussi ces théorèmes. Il suffit de savoir que le nombre a des classes ambiges de k est toujours $\leqslant 2^{r-1}$. Ce fait se déduit du théorème 106 relatif au nombre des classes ambiges qui proviennent d'idéaux ambiges, en tenant compte des conclusions de la deuxième et de la troisième partie du théorème 107; ces déductions sont tout à fait indépendantes du théorème 102.

Soit alors, comme avant, f le nombre des classes du genre principal, g le nombre des genres et f' le nombre de f classes du genre principal qui sont des carrés de classes. Il en résulte, comme au paragraphe 78, que $gf = af'$, et comme, d'autre part, $g = 2^{r-1}$, de plus $a \leqslant 2^{r-1}$, il faut que $f' \leqslant f$, et, par suite, $f' = f$, $a = 2^{r-1}$.

La première égalité démontre le théorème 103; la seconde, le théorème 108, et, par suite, le théorème 102 pour $n = -1$.

Le théorème 102 résulte complètement de 103 et des derniers résultats. Car le nombre n en question, en vertu des conditions qui lui sont imposées, est alors la norme d'un idéal $\mathfrak{h}$ du genre principal, précédé du signe prévu au paragraphe 65. Désignons par $\mathfrak{j}$ un idéal tel que $\mathfrak{h} \sim \mathfrak{j}^2$; il faut que $\alpha = \dfrac{\mathfrak{h}\, n(\mathfrak{j})}{\mathfrak{j}^2}$, soit un nombre entier ou fractionnaire du corps k, et l'on a $n(\alpha) = \pm n$, d'où le théorème 102, si l'on considère qu'il est vrai pour $n = -1$.

Nous voyons, en somme, que la méthode transcendante nous permet de démontrer les résultats des paragraphes 71-78 dans l'ordre inverse où les avons trouvés par la voie arithmétique.

§ 83. — Le sens plus étroit de l'équivalence et du concept de classes.

Si nous prenons pour base de l'équivalence de deux idéaux le sens plus étroit exposé au paragraphe 24, les théorèmes établis aux chapitres XVII, XVIII subissent de légères modifications faciles à trouver.

Il est tout d'abord évident que le sens plus étroit de l'équivalence coïncide avec le sens ordinaire dans tous les cas pour un corps imaginaire k, et pour un corps réel k lorsque la norme de l'unité fondamentale ε, $n(\varepsilon) = -1$. Mais lorsque dans un corps réel $n(\varepsilon) = +1$, une classe idéale au sens de la répartition primitive se répartit ici en

deux classes; en particulier, la classe des idéaux principaux se décomposera ici en deux classes représentées par l'idéal principal (1) et par l'idéal principal $(\sqrt{m})$. Soit h' le nombre des classes d'idéaux avec le sens plus étroit de l'équivalence; on a, dans les circonstances actuelles, $h'=2h$. [Dedekind [1].]

§ 84. — Le théorème fondamental pour le nouveau concept de classe et de genre.

Au sens nouveau de classe correspond un sens nouveau de genre. Le genre d'un idéal $\mathfrak{j}$ du corps $k(\sqrt{m})$ sera dorénavant défini dans tous les cas par les t unités :

$$\left(\frac{+n(\mathfrak{j}), m}{l_1}\right), \ldots, \left(\frac{+n(\mathfrak{j}), m}{l_t}\right).$$

Ici, la norme de $\mathfrak{j}$ sera constamment prise avec le signe +. Pour un corps imaginaire, ce sens nouveau de l'équivalence coïncide totalement avec l'ancien. On peut en dire autant d'un corps réel k, dans le cas où le système de caractères de -1 n'est composé que d'unités positives. Cette dernière circonstance se présente toujours lorsque dans le corps la norme de l'unité fondamentale est égale à -1. Supposons donc k réel et la norme de l'unité fondamentale égale à $+1$; il faut distinguer deux cas, suivant que le système de caractères de -1 se compose uniquement d'unités positives ou non.

Dans le premier cas, les idéaux (1) et $\mathfrak{a}=(\sqrt{m})$ appartiennent tous deux au même genre, car

$$\left(\frac{n(\mathfrak{a}), m}{l_i}\right)=\left(\frac{+m, m}{l_i}\right)=\left(\frac{+m, m}{l_i}\right)\left(\frac{-1, m}{l_i}\right)=\left(\frac{-m, m}{l_i}\right)=+1,$$

pour $i=1, \ldots, t$.

Les nouveaux genres comprennent les mêmes classes que les anciens, et le nombre des genres est 2^{t-1}.

Dans le second cas, les deux classes d'idéaux représentés par l'idéal (1) et l'idéal $\mathfrak{a}=(\sqrt{m})$ appartiennent à deux genres différents des genres nouveaux. Le nombre des genres nouveaux est double de celui des anciens; mais en ce qui concerne ce cas, le nombre des caractères au sens primitif du genre était $t-1$, et le nombre de ces genres 2^{t-2}, tandis que le nombre des nouveaux genres est comme dans les autres cas 2^{t-1}. Et comme dans tous les cas le produit

$$\left(\frac{-1, m}{l_1}\right) \cdots \left(\frac{-1, m}{l_t}\right)=+1,$$

le théorème fondamental 100 est vrai aussi en tenant compte du sens nouveau de classes et de genre à la condition d'y écrire t au lieu de r.

Les autres propositions et démonstrations des chapitres XVII et XVIII se modifient de même sans difficulté, et même quelques théorèmes s'énoncent plus simplement.

CHAPITRE XIX.

La détermination du nombre des classes d'idéaux du corps quadratique.

§ 85. — Le symbole $\left(\frac{a}{n}\right)$ pour un nombre composé n.

On obtient une expression remarquable du nombre h des classes d'idéaux du corps quadratique k par la formule du théorème 109, en transformant par le calcul le nombre

$$\mathop{\mathrm{L}}_{s=1} \prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}}$$

en un nombre fini.

Pour cela, il nous faut d'abord définir le symbole $\left(\frac{a}{n}\right)$, aussi pour le cas où n est un nombre entier positif rationnel composé. Soit $n = pq \ldots w$, où $p, q, \ldots, w$ sont des nombres premiers rationnels égaux ou distincts ; nous définirons

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p}\right)\left(\frac{a}{q}\right)\cdots\left(\frac{a}{w}\right);$$

de plus, soit $\left(\frac{a}{1}\right)=+1$; on a, pour $s>1$,

$$\prod_{(p)} \frac{1}{1-\left(\frac{d}{p}\right)p^{-s}} = \sum_{(n)} \left(\frac{d}{n}\right)\frac{1}{n^s},$$

où la somme s'étend à tous les entiers positifs rationnels. Le calcul de la limite de cette somme pour $s=1$ nous donne un nombre fini pour le nombre des classes h.

Le résultat est donné par le théorème suivant.

§ 86. — L'expression finie donnant le nombre de classes d'idéaux.

Théorème 114. — Le nombre h des classes d'idéaux du corps $k(\sqrt{m})$ est

$$h = \frac{-w}{2|d|}\sum_{(n)}\left(\frac{d}{n}\right)n, \qquad \text{pour } m<0,$$

$$h = \frac{1}{2\log\varepsilon}\log\frac{\prod_{(b)}\left(e^{\frac{bi\pi}{d}}-e^{-\frac{bi\pi}{d}}\right)}{\prod_{(a)}\left(e^{\frac{ai\pi}{d}}-e^{-\frac{ai\pi}{d}}\right)}, \qquad \text{pour } m>1.$$

où la somme $\sum\limits_{(n)}$ s'étend aux $|d|$ entiers rationnels $n=1, 2, \ldots |d|$ et où les produits $\prod\limits_{(a)}$, $\prod\limits_{(b)}$ s'étendent à tous les nombres a et b parmi ces $|d|$ nombres satisfaisant à $\left(\frac{d}{a}\right) = +1$ et $\left(\frac{d}{b}\right) = -1$. [Dirichlet[8, 9]; Weber[1].]

Démonstration. — Soient n et n' deux nombres positifs. Lorsque n et d ont un diviseur commun $\neq \pm 1$ $\left(\frac{d}{n}\right) = 0$. Par contre, lorsque n est premier avec d, on voit facilement que $\left(\frac{d}{n}\right) = \prod\limits_{(w)}\left(\frac{d,\,n}{w}\right)$, où le produit s'étend à tous les nombres premiers w qui divisent n. D'après le lemme 14, $\prod\limits_{(l)}\left(\frac{d,\,n}{l}\right)$ représente la même unité lorsque l parcourt toutes les valeurs des nombres premiers contenus dans d. Soit $n' \equiv n$ suivant d

$$\prod_{(l)}\left(\frac{d,\,n}{l}\right) = \prod_{(l)}\left(\frac{d,\,n'}{l}\right),$$

d'où

$$\left(\frac{d}{n}\right) = \left(\frac{d}{n'}\right), \qquad \text{si } n \equiv n',\ (d). \tag{29}$$

De plus, on a

$$\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \ldots + \left(\frac{d}{d}\right) = 0, \tag{30}$$

car nous pouvons déterminer un nombre b tel que $\left(\frac{d}{b}\right) = -1$ et on a, en tenant compte de (29) :

$$\left(\frac{d}{b}\right) + \left(\frac{d}{2b}\right) + \ldots + \left(\frac{d}{db}\right) = -\left\{\left(\frac{d}{1}\right) + \left(\frac{d}{2}\right) + \ldots + \left(\frac{d}{d}\right)\right\}.$$

La formule

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)}\int_0^{\infty} e^{-nt}\, t^{s-1}\, dt$$

donne, en tenant compte de la règle 29,

$$\mathrm{L}_{s=1} \sum_{(n)} \left(\frac{d}{n}\right)\frac{1}{n^s} = \mathrm{L}_{s=1} \int_0^{\infty} \frac{F(e^{-t})\, t^{s-1}}{1-e^{-dt}}\, dt,$$

où l'on a posé

$$F(x) = \left(\frac{d}{1}\right)x + \left(\frac{d}{2}\right)x^2 + \ldots \left(\frac{d}{d}\right)x^d.$$

L'égalité 30 nous montre que $F(x)$ admet le facteur $1-x$, et la fonction rationnelle $\frac{F(e^{-t})}{1-e^{-dt}}$ est finie pour $t=0$.

Aussi

$$\lim_{s=1} \int_0^\infty \frac{F(e^{-t})\, t^{s-1}}{1-e^{-dt}}\, dt = \int_0^\infty \frac{F(e^{-t})}{1-e^{-dt}}\, dt;$$

faisons le changement de variable $x = e^{-t}$, on a

$$\int_0^1 \frac{F(x)}{x(1-x^d)}\, dx,$$

et la décomposition en fractions simples donne

$$\frac{F(x)}{x(1-x^d)} = -\frac{1}{d} \sum_{(n)} \frac{F\left(e^{\frac{2ni\pi}{d}}\right)}{x - e^{\frac{2ni\pi}{d}}},$$

où la somme s'étend à $n = 1, 2, \ldots |d|$, et, d'après un théorème de Gauss, $F\left(e^{\frac{2ni\pi}{d}}\right)$, c'est-à-dire

$$\sum_{n'} \left(\frac{d}{n'}\right) e^{\frac{2nn'i\pi}{d}} = \left(\frac{d}{n}\right) \sqrt{d};$$

n' prend encore les valeurs $1, 2, \ldots, |d|$, et $\sqrt{d}$ est positif pour d positif, imaginaire positif pour d négatif [voir § 124]. Comme, de plus,

$$\int_0^1 \frac{dx}{x - e^{\frac{2ni\pi}{d}}} = \log \frac{e^{\frac{ni\pi}{|d|}} - e^{-\frac{ni\pi}{|d|}}}{i} - \frac{i\pi}{|d|}\left(n - \tfrac{1}{2} d\right),$$

où il faut prendre la valeur réelle du logarithme, on en tire sans difficulté le résultat du théorème 114.

La forme de ce résultat est essentiellement différente, suivant que le corps est imaginaire ou réel. Dans le premier cas, h peut être déduit de la formule indiquée sans plus. Dans le second cas, il faut d'abord connaître l'unité fondamentale ε; le quotient des deux produits $\prod_{(a)}$ et $\prod_{(b)}$ est, on le montrera au paragraphe 121, une certaine unité du corps quadratique provenant de la théorie de la division du cercle.

Prenons comme exemple le cas d'un corps imaginaire, soit $m = -p$, et p un nombre rationnel premier positif $\equiv 3$ suivant 4 et > 3; on a

$$h = \frac{\Sigma b - \Sigma a}{p};$$

ici, Σa, Σb désigne l'un la somme des restes quadratiques suivant p, l'autre la somme des non-restes compris entre o et p. Une transformation simple permet de faire disparaître le dénominateur p de cette expression. On voit alors que le nombre des classes h est égal à l'excès du nombre des restes quadratiques de p situés entre o et $\frac{p}{2}$ sur le nombre des non-restes compris entre les mêmes limites, ou au tiers de cette différence, suivant que $p \equiv 7$ ou $\equiv 3$ suivant 8. Le premier nombre excède donc le second, ce qui n'a pas encore été démontré par une voie purement arithmétique.

§ 57. — Le corps de nombres biquadratiques de Dirichlet.

Le problème suivant est une généralisation de la théorie du corps quadratique qui vient d'être développée. Au lieu de prendre comme base le domaine de rationalité formé par tous les nombres naturels rationnels, nous prendrons comme base le domaine de rationalité formé par un corps quadratique k; et nous examinerons les corps K quadratiques relatifs par rapport à k, c'est-à-dire les corps biquadratiques K qui admettent le corps donné k comme sous-corps.

Lorsque le corps k est déterminé par l'unité imaginaire $\sqrt{-1}$, le corps K sera dit *le corps biquadratique de Dirichlet*. On possède des recherches étendues pour ce corps. [Dirichlet[10, 11, 12], Eisenstein[5, 6], Bachmann[1, 3], Minnigerode[1], Hilbert[4].] Le théorème 100 s'applique encore à la répartition correspondante des idéaux du corps K en genres; ce théorème s'applique avec une transformation appropriée et les deux méthodes de démonstration du chapitre XVIII peuvent être employées dans le corps K, de sorte que ce théorème fondamental pour le corps quadratique de Dirichlet peut être établi aussi bien sur une base purement arithmétique [Hilbert[4]] qu'au moyen de la méthode transcendante de Dirichlet [Dirichlet[10, 11, 12], Minnigerode[1]].

Si le corps K contient, outre le corps quadratique $\sqrt{-1}$, deux autres corps quadratiques $k(\sqrt{+m})$ et $k(\sqrt{-m})$, présente un intérêt particulier. Pour un pareil *corps spécial de Dirichlet* K, on a le fait suivant, auquel on parvient encore par la voie transcendante ou par la voie purement arithmétique.

Théorème 116. — Le nombre des classes d'idéaux d'un corps spécial biquadratique de Dirichlet $K(\sqrt{+m}, \sqrt{-m})$ est le produit du nombre des classes dans les corps quadratiques $k(\sqrt{+m})$ et $k(\sqrt{-m})$ ou la moitié de ce produit, suivant que la norme relative par rapport à $k(\sqrt{-1})$ de l'unité fondamentale du corps K est égale à $\pm i$ ou à ± 1. Dirichlet désigne ce théorème comme l'un des plus beaux de la théorie des imaginaires et il le trouve surprenant, parce qu'il révèle un rapport entre les deux corps quadratiques déterminés par la racine de deux nombres opposés.

La démonstration arithmétique de ce théorème permet, et cela d'une façon très simple, de distinguer au moyen de certaines conditions remplies par les caractères du genre les classes d'idéaux des corps biquadratiques $K(\sqrt{+m}, \sqrt{-m})$ qui peuvent être considérées comme le produit d'une classe d'idéaux de $k(\sqrt{+m})$ et d'une d'une classe d'idéaux de $k(\sqrt{-m})$. [Hilbert[4].]

CHAPITRE XX.

Les anneaux de nombres et les modules du corps quadratique.

§ 88. — Les anneaux de nombres du corps quadratique.

La théorie des anneaux et des modules d'un corps quadratique s'obtient rapidement en particularisant les théorèmes généraux du chapitre IX. On s'aperçoit facilement que tout anneau du corps est obtenu au moyen d'un seul nombre de la forme $f\omega$, où ω est le nombre défini au paragraphe 59, celui qui forme avec 1 une base du corps k, où f est un certain nombre entier rationnel, le conducteur de l'anneau. Si, de plus, d est négatif et < -4, le théorème 66 nous apprend que le nombre h_r des classes régulières de l'anneau r est donné par la formule

$$h_r = hf \prod_{(p)} \left(1 - \left(\frac{d}{p}\right) \frac{1}{p} \right),$$

où le produit s'étend à toutes les valeurs des entiers rationnels premiers p contenus dans f. [Dedekind[1, 3].]

§ 89. — Un théorème relatif aux classes de modules du corps quadratique. Les formes quadratiques binaires.

Théorème 116. — Dans une classe de modules du corps quadratique k, il y a toujours des idéaux d'anneaux réguliers. [Dedekind[1].]

Démonstration. — Soit $[\mu_1, \mu_2]$ un module quelconque du corps k, où μ_1 et μ_2 sont des nombres entiers, et soit $\partial = f^2 d$ et le discriminant de la classe de modules déterminée par $[\mu_1, \mu_2]$; de plus, désignons par $\mathfrak{m} = (\mu_1, \mu_2)$ l'idéal déterminé par les nombres μ_1 et μ_2, et soit $s\mathfrak{m} = \mathfrak{m}'$ l'idéal conjugué de $\mathfrak{m}$. Déterminons un entier du corps k, α, divisible par $\mathfrak{m}'$ et tel que $\frac{\alpha}{\mathfrak{m}'}$ soit premier avec ∂. Posons alors

$$\alpha_1 = \frac{\alpha\mu_1}{n(\mathfrak{m})}, \qquad \alpha_2 = \frac{\alpha\mu_2}{n(\mathfrak{m})};$$

alors $[\alpha_1, \alpha_2]$ sera un module équivalent à $[\mu_1, \mu_2]$, alors que l'idéal $\mathfrak{a} = (\alpha_1, \alpha_2)$ est premier avec ∂.

Supposons δ pair, nous considérerons d'abord les trois entiers α_1, α_2, $\alpha_1+\alpha_2$; parmi ces nombres, l'un au moins est premier avec 2, sans quoi, parmi ces trois nombres, deux au moins auraient un diviseur idéal commun avec 2, ce qui est contraire à l'hypothèse que l'idéal $\mathfrak{a}$ est premier avec δ. Soit α_1 premier avec 2. Désignons par $p, q, r, \ldots, w$ les facteurs premiers rationnels impairs de δ. Comme $\mathfrak{a}$ est premier avec p, il faut que l'un au moins des trois nombres α_1, $\alpha_1+\alpha_2$, $\alpha_1+2\alpha_2$ soit premier avec p. Supposons $\alpha_1+x\alpha_2$ premier avec p, $\alpha_1+y\alpha_2$ premier avec q, où $x, y, \ldots$ sont des entiers rationnels. Il en résultera facilement l'existence d'un entier rationnel a, tel que $\alpha_1+a\alpha_2$ soit premier avec δ.

Posons alors

$$b=\frac{|n(\alpha_1+a\alpha_2)|}{n(\mathfrak{a})},\qquad \beta=\frac{\alpha_2(\alpha_1'+a\alpha_2')}{n(\mathfrak{a})},$$

où α_1', α_2' sont les nombres conjugués de α_1, α_2; alors b est un entier rationnel positif et β un entier algébrique, et le module $[\alpha_1, \alpha_2]=[\alpha_1+a\alpha_2, \alpha_2]$ est équivalent au module $[b, \beta]$, et, en même temps, comme $(b, \beta)=\frac{\alpha_1'+a\alpha_2'}{\mathfrak{a}'}$, la norme $N(b, \beta)=b$. Le module $[b, \beta]$ est évidemment un idéal d'anneau régulier de l'anneau r déterminé par le nombre β, $r=(\beta)$; le théorème 116 est complètement démontré.

A cause de

$$\delta=\frac{1}{[n(b,\beta)]^2}\begin{vmatrix} b, & \beta \\ b, & \beta' \end{vmatrix}^2=\begin{vmatrix} 1, & \beta \\ 1, & \beta' \end{vmatrix}^2,$$

le discriminant de l'anneau r est égal au discriminant de la classe de module considérée. L'anneau r est le seul qui offre parmi ses idéaux d'anneau réguliers des modules équivalents à $[\mu_1, \mu_2]$. Le théorème 116 nous montre que, pour le corps quadratique, cela revient au même de considérer les classes de modules ou les classes d'anneaux réguliers.

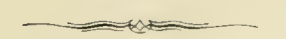
D'après les raisonnements des paragraphes 30 et 35, on voit qu'à chaque classe de modules d'un corps quadratique $k(\sqrt{m})$ correspond une classe de formes binaires quadratiques à coefficients entiers et rationnels, et, réciproquement, à chaque pareille classe de formes dont le discriminant n'est pas un carré, correspond une classe de modules d'un corps quadratique, où les classes de modules et les formes ont même discriminant. Nous avons complètement terminé les recherches sur les corps quadratiques de discriminant donné δ.

§ 90. La théorie inférieure et la théorie supérieure du corps quadratique.

Les recherches faites dans la troisième partie de ce livre forment la théorie inférieure du corps quadratique; je désigne par *théorie supérieure* les propriétés du corps

quadratique qui nécessitent, pour les établir, l'emploi de corps auxiliaires de degré plus élevé. On trouvera un chapitre relatif à cette théorie dans la quatrième partie.

Pour construire la théorie d'un corps de classe relatif à un corps imaginaire quadratique et du corps relatif abélien correspondant, il faut le secours de la multiplication complexe des fonctions elliptiques, et ceci est un obstacle qui m'a empêché d'introduire cette étude dans mon rapport.



THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

MÉMOIRE de M. DAVID HILBERT,

Professeur à l'Université de Gœttingen.

PUBLIÉ PAR LA SOCIÉTÉ

DEUTSCHE MATHEMATIKER VEREINIGUNG, en 1897.

TRADUIT PAR M. Th. GOT.

Ancien Ingénieur de la Marine,

Agrégé des Sciences mathématiques.

QUATRIÈME PARTIE.

LES CORPS CIRCULAIRES.

CHAPITRE XXI.

Les racines de l'unité d'indice premier l et le corps circulaire qu'elles définissent.

§ 91. — DEGRÉ DU CORPS CIRCULAIRE DES $l^{\text{ièmes}}$ RACINES DE L'UNITÉ ET DÉCOMPOSITION DU NOMBRE PREMIER l DANS CE CORPS.

Soit l un nombre premier impair et $\zeta = e^{\frac{2i\pi}{l}}$. L'équation de degré l

$$x^l - 1 = 0$$

a les l racines

$$\zeta, \zeta^2, \ldots\ldots, \zeta^{l-1}, \zeta^l = 1.$$

Ces nombres sont les *racines $l^{\text{ièmes}}$ de l'unité*. Le corps qu'elles définissent, $c(\zeta)$, s'appellera le *corps circulaire* des racines $l^{\text{ièmes}}$ de l'unité. On a d'abord la proposition suivante :

THÉORÈME 117. — Le degré du corps $c(\zeta)$ est $l-1$. Le nombre premier l admet dans $c(\zeta)$ la décomposition $l=\mathfrak{l}^{l-1}$, $\mathfrak{l}$ étant l'idéal premier du premier degré $(1-\zeta)$.

Démonstration. — Le nombre ζ vérifie l'équation

$$F(x)=\frac{x^l-1}{x-1}=x^{l-1}+x^{l-2}+\ldots+1=0,$$

le degré du corps est donc au plus $l-1$; $\zeta, \zeta^2, \ldots, \zeta^{l-1}$ étant les $l-1$ racines de cette équation, on a identiquement en x :

$$x^{l-1}+x^{l-2}+\ldots+1=(x-\zeta)(x-\zeta^2)\ldots(x-\zeta^{l-1}).$$

D'où, pour $x=1$,

(31) $$l=(1-\zeta)(1-\zeta^2)\ldots(1-\zeta^{l-1}).$$

Soit maintenant g un entier quelconque >1 non divisible par l, et soit g' un entier positif tel que $gg'\equiv 1 \bmod l$. Alors les quotients

$$\frac{1-\zeta^g}{1-\zeta}=1+\zeta+\zeta^2+\ldots+\zeta^{g-1},$$

et

$$\frac{1-\zeta}{1-\zeta^g}=\frac{1-\zeta^{gg'}}{1-\zeta^g}=\frac{1-(\zeta^g)^{g'}}{1-\zeta^g}=1+\zeta^g+\zeta^{2g}+\ldots+\zeta^{(g'-1)g}$$

sont deux entiers algébriques, et par suite

$$\varepsilon_g=\frac{1-\zeta^g}{1-\zeta}$$

est une unité du corps $c(\zeta)$. Si nous posons de plus $\lambda=1-\zeta$ et $\mathfrak{l}=(\lambda)$, la formule (31) prend la forme

(32) $$l=\lambda^{l-1}\varepsilon_2\varepsilon_3\ldots\varepsilon_{l-1}=\mathfrak{l}^{l-1}.$$

On conclut immédiatement du théorème 33 qu'un nombre premier rationnel ne peut, dans un corps donné, être le produit d'un nombre d'idéaux premiers supérieur au degré du corps. Le degré du corps $c(\zeta)$ doit donc, vu la formule (32), être au moins égal à $l-1$; d'après ce qui précède, il est donc exactement égal à $l-1$. D'autre part, pour la même raison, l'idéal $\mathfrak{l}$ doit être indécomposable dans $c(\zeta)$ et, par suite, c'est un idéal premier. [Dedekind[1].]

Ce résultat montre en même temps que le polynome $F(x)$ est irréductible dans le domaine des nombres rationnels.

§ 92. — Base et discriminant du corps circulaire.

Théorème 118. — Dans le corps $c(\zeta)$ les nombres

$$1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{l-2}$$

forment une base. Le discriminant du corps est

$$d = (-1)^{\frac{l-1}{2}}\, l^{l-2}.$$

Démonstration. — La différente du nombre ζ dans le corps $c(\zeta)$ est

$$\delta = (\zeta - \zeta^2)(\zeta - \zeta^3)\ldots(\zeta - \zeta^{l-1}) = \left[\frac{d\,\mathrm{F}(x)}{dx}\right]_{x=\zeta}.$$

De

$$(x-1)\,\mathrm{F}(x) = x^l - 1$$

on tire

$$(x-1)\frac{d\mathrm{F}(x)}{dx} + \mathrm{F}(x) = l x^{l-1}, \text{ donc } \delta = -\frac{l\zeta^{l-1}}{1-\zeta};$$

d'après la remarque faite au paragraphe 3, le discriminant du nombre ζ est alors

$$d(\zeta) = (-1)^{\frac{(l-1)(l-2)}{2}}\, n(\delta) = (-1)^{\frac{l-1}{2}}\, l^{l-2}.$$

Comme le discriminant $d(\lambda)$ du nombre λ a certainement la même valeur $d(\zeta)$, la remarque faite pour la formule (1) dans la démonstration du théorème 5, paragraphe 3, montre que tout entier α du corps $c(\zeta)$ peut être mis sous la forme

$$\alpha = \frac{a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2}}{l^{l-2}}, \tag{33}$$

$a_0,\ a_1,\ \ldots,\ a_{l-2}$ étant des entiers rationnels.

Les nombres $a_0,\ a_1,\ \ldots,\ a_{l-2}$ doivent alors nécessairement être tous divisibles par le dénominateur l^{l-2}. Pour montrer d'abord qu'ils sont divisibles une fois par l, supposons qu'il y en ait de non divisibles par l et soit a_q le premier; de $l^{l-2}\alpha \equiv 0$, mod l résulterait alors, vu $l = \mathfrak{l}^{l-1}$, $a_q\lambda^q \equiv 0$, mod $\mathfrak{l}^{q+1}$, c'est-à-dire $a_q \equiv 0$, mod $\mathfrak{l}$, et par suite aussi mod l contrairement à l'hypothèse. On peut donc supprimer un facteur l au numérateur et au dénominateur de (33). En poursuivant cette simplification, on voit finalement que tout entier α du corps $c(\zeta)$, dans ses représentations

$$\alpha = a_0 + a_1\lambda + \ldots + a_{l-2}\lambda^{l-2} = b_0 + b_1\zeta + \ldots + b_{l-2}\zeta^{l-2}$$

avec des coefficients rationnels $a_0,\ a_1,\ \ldots,\ a_{l-2}$ ou $b_0,\ b_1,\ \ldots,\ b_{l-2}$, admet pour tous ces derniers des valeurs entières.

Puisque les puissances $1,\ \zeta,\ \ldots,\ \zeta^{l-2}$ du nombre ζ forment donc une base du corps $c(\zeta)$, le discriminant $d(\zeta)$ du nombre ζ est en même temps le discriminant du corps.

§ 93. Décomposition des nombres premiers différents de l.

La décomposition du nombre premier l dans $c(\zeta)$ a été donnée dans le théorème 117. Pour celle des autres nombres premiers, on a la règle suivante :

Théorème 119. — p étant un nombre premier différent de l et f le plus petit exposant positif pour lequel $p^f \equiv 1$, mod l, si l'on pose $l-1=ef$, on a dans $c(\zeta)$ la décomposition

$$p = \mathfrak{p}_1 \dots \mathfrak{p}_e$$

où $\mathfrak{p}_1, \dots, \mathfrak{p}_e$ sont des idéaux premiers distincts de degré f de $c(\zeta)$. [Kummer [illegible].]

Démonstration. Soit $\alpha = a + a_1\zeta + \dots + a_{l-2}\zeta^{l-2}$ un entier arbitraire de $c(\zeta)$; on a les congruences

$$\alpha^p \equiv (a + a_1\zeta + \dots + a_{l-2}\zeta^{l-2})^p \equiv a + a_1\zeta^p + \dots + a_{l-2}\zeta^{p(l-2)} \quad (\text{mod } p),$$

$$\alpha^{p^2} \equiv (a + a_1\zeta^p + \dots + a_{l-2}\zeta^{p(l-2)})^p \equiv a + a_1\zeta^{p^2} + \dots + a_{l-2}\zeta^{p^2(l-2)} \quad (\text{mod } p),$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\alpha^{p^f} \equiv (a + a_1\zeta^{p^{f-1}} + \dots + a_{l-2}\zeta^{p^{f-1}(l-2)})^p \equiv a + a_1\zeta^{p^f} + \dots + a_{l-2}\zeta^{p^f(l-2)} \equiv \alpha \quad (\text{mod } p).$$

Si maintenant $\mathfrak{p}$ est un idéal premier divisant p, la congruence $\alpha^{p^f} \equiv \alpha$ (mod p) est vérifiée *a fortiori* mod $\mathfrak{p}$, c'est-à-dire la congruence

$$(34) \qquad \xi^{p^f} - \xi \equiv 0, \quad (\mathfrak{p}),$$

est vérifiée par n'importe quel entier de $c(\zeta)$. Le nombre des racines de cette congruence incongrues mod $\mathfrak{p}$ est par suite égal au nombre des entiers de c incongrus mod $\mathfrak{p}$, c'est-à-dire à $n(\mathfrak{p}) = p^{f'}$, f' désignant le degré de l'idéal premier $\mathfrak{p}$; mais le degré de la congruence (34) est p^f. On a donc (théorème 26) $p^{f'} \leqslant p^f$, c'est-à-dire $f' \leqslant f$.

D'autre part, vu le théorème de Fermat généralisé (théorème 24), on a sûrement

$$(35) \qquad \zeta^{p^{f'}-1} \equiv 1, \quad (\mathfrak{p}).$$

Comme, vu la formule (31), pour un exposant g non divisible par l le nombre $1-\zeta^g$ est toujours premier à $\mathfrak{p}$, il résulte de la congruence (35) $p^{f'} - 1 \equiv 0$, mod l, et par suite $f' \geqslant f$. Donc $f' = f$, c'est-à-dire que tout idéal premier diviseur de p est de degré f.

Comme p ne divise pas le discriminant du corps $c(\zeta)$, il résulte du théorème 31 que p se décompose en idéaux premiers tous distincts. En posant $p = \mathfrak{p}_1 \dots \mathfrak{p}_{e'}$, on a $n(p) = p^{l-1} = p^{e'f}$, c'est-à-dire $l-1 = e'f$, $e' = e$. La démonstration du théorème 119 est ainsi complète.

Pour obtenir effectivement les idéaux premiers $\mathfrak{p}_1, \ldots, \mathfrak{p}_e$, appliquons le théorème 33, en ayant égard à la remarque faite à ce sujet paragraphe 13. On a, d'après cela, la décomposition identique mod p

$$F_l(x) \equiv F_1(x) F_2(x) \ldots F_e(x), \qquad (p),$$

où $F_1(x), \ldots, F_e(x)$ sont des polynomes entiers de degré f à coefficients entiers, irréductibles et incongrus mod p. Ces fonctions une fois déterminées, on obtient la représentation cherchée par les formules

$$\mathfrak{p}_1 = \big(p, F_1(\zeta)\big), \ldots, \mathfrak{p}_e = \big(p, F_e(\zeta)\big) \text{ [1]}.$$

CHAPITRE XXII.

Racines $m^{\text{ièmes}}$ de l'unité, m étant composé, et corps circulaire correspondant.

§ 94. — Le corps des racines $m^{\text{ièmes}}$ de l'unité.

Soit m un nombre entier positif quelconque et posons $Z = e^{\frac{2i\pi}{m}}$. L'équation de degré m

$$x^m - 1 = 0$$

a les racines

$$Z, \quad Z^2, \quad \ldots, \quad Z^{m-1}, \quad Z^m = 1.$$

Ces nombres sont les *racines* $m^{\text{ièmes}}$ *de l'unité*; elles définissent un corps $c(Z)$, appelé le *corps circulaire* des racines $m^{\text{ièmes}}$ de l'unité.

Si m est composé, on a

$$m = l_1^{h_1} l_2^{h_2} \ldots,$$

$l_1, l_2, \ldots$ étant les facteurs premiers distincts de m, et l'on peut décomposer $\frac{1}{m}$ en fractions simples :

$$\frac{1}{m} = \frac{a_1}{l_1^{h_1}} + \frac{a_2}{l_2^{h_2}} + \ldots,$$

où $a_1, a_2, \ldots$ sont des entiers positifs ou négatifs et où a_1 est premier à l_1, a_2 à l_2, etc.

---

(1) N. T. — Dans le cas particulier de $f = 1$, c'est-à-dire de $p = ml + 1$, on a, en désignant par g une racine primitive mod p :

$$F(x) \equiv (x - g^m)(x - g^{2m}) \ldots (x - g^{(l-1)m}) \qquad (\text{mod } p),$$

et, par suite,

$$\mathfrak{p}_1 = (p, \zeta - g^m), \quad \mathfrak{p}_2 = (p, \zeta - g^{2m}), \quad \ldots, \quad \mathfrak{p}_{l-1} = (p, \zeta - g^{(l-1)m}).$$

De là résulte

$$Z = Z_1^{a_1} Z_2^{a_2} \ldots,$$

en posant

$$Z_1 = e^{\frac{2i\pi}{l_1^{h_1}}}, \quad Z_2 = e^{\frac{2i\pi}{l_2^{h_2}}} \quad \ldots.$$

Le corps $c(Z)$ résulte donc de la combinaison des corps $c(Z_1)$ des racines $l_1^{h_1}$ ièmes de l'unité, $c(Z_2)$, etc. Nous commencerons donc par traiter le cas le plus simple, où $m = l^h$ ne contient qu'un nombre premier.

§ 95. — Degré du corps circulaire des l^h ièmes racines de l'unité et décomposition du nombre premier l dans ce corps.

Théorème 120. — Que l soit égal à 2 ou à un nombre premier impair, le degré du corps $c(Z)$, $Z = e^{\frac{2i\pi}{l^h}}$, est égal à $l^{h-1}(l-1)$. Le nombre premier l se décompose dans $c(Z)$ en $l = \mathfrak{L}^{l^{h-1}(l-1)}$, $\mathfrak{L}$ étant un idéal du premier degré du corps.

Démonstration. — Z vérifie l'équation de degré $l^{h-1}(l-1)$

$$F(x) = \frac{x^{l^h} - 1}{x^{l^{h-1}} - 1} = x^{l^{h-1}(l-1)} + x^{l^{h-1}(l-2)} + \ldots + 1 = 0.$$

Si l'on désigne par g un entier non divisible par l et g' un entier tel que $gg' \equiv 1$ mod l^h, on voit, comme au paragraphe 91, que

$$E_g = \frac{1 - Z^g}{1 - Z},$$

ainsi que l'inverse

$$\frac{1 - Z}{1 - Z^g} = \frac{1 - Z^{gg'}}{1 - Z^g},$$

sont des entiers du corps; par suite E_g est une unité. On en déduit, comme au paragraphe 91, les égalités

$$F(1) = l = \prod_{(g)} (1 - Z^g) = \Lambda^{l^{h-1}(l-1)} \prod_{(g)} E_g = \mathfrak{L}^{l^{h-1}(l-1)},$$

où $\Lambda = 1 - Z$, $\mathfrak{L} = (\Lambda)$ et où les produits doivent être étendus à tous les entiers positifs premiers à l et $< l^h$.

On en conclut, comme paragraphe 91, que le degré du corps est au moins égal à $l^{h-1}(l-1)$ et a, par suite, exactement cette valeur.

§ 96. — Base et discriminant du corps circulaire des l^h ièmes racines de 1.

Théorème 121. — Dans le corps circulaire $c(Z)$, $Z = e^{\frac{2i\pi}{l^h}}$, une base est formée par les nombres

$$1, \quad Z, \quad Z^2, \quad \ldots, \quad Z^{l^{h-1}(l-1)-1}.$$

Le discriminant du corps est

$$d = \pm\, l^{l^{h-1}(hl-h-1)},$$

avec le signe — pour $l^h = 4$ ou $l \equiv 3 \bmod 4$, avec le signe + dans les autres cas.

Théorème 122. — p étant un nombre premier différent de l et f étant le plus petit exposant positif pour lequel $p^f \equiv 1$, mod l^h, si l'on pose $l^{h-1}(l-1) = ef$, on a la décomposition

$$p = \mathfrak{P}_1 \ldots \mathfrak{P}_e,$$

où $\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ sont des idéaux premiers distincts de degré f.

Démonstration analogue à celle des théorèmes 118 et 119.

§ 97. — Le corps circulaire général. Degré, discriminant, idéaux premiers.

Soit maintenant m un produit de puissances de nombres premiers distincts $m = l_1^{h_1}\, l_2^{h_2} \ldots$. Le corps $c(Z)$ des $m$ièmes racines de l'unité est, comme on l'a vu, le résultat de la composition des corps $c(Z_1)$, $c(Z_2)$, ... des racines $l_1^{h_1}$, $l_2^{h_2}$, ... èmes de l'unité. Comme les discriminants de ces derniers sont premiers entre eux, on déduit immédiatement du théorème 87 (§ 52) la proposition :

Théorème 123. — Le degré du corps $c(Z)$ des racines $m = l_1^{h_1}\, l_2^{h_2} \ldots$ ièmes de l'unité est

$$\Phi(m) = l_1^{h_1-1}(l_1 - 1)\, l_2^{h_2-1}(l_2 - 1) \ldots .$$

En appliquant la deuxième partie du théorème 88 et ayant égard au théorème 121, on obtient la proposition :

Théorème 124. — Le corps circulaire $c(Z)$ des $m$ièmes racines de l'unité a pour base

$$1, \quad Z, \quad Z^2, \quad \ldots, \quad Z^{\Phi(m)-1}.$$

Le discriminant du corps $c(Z)$ s'obtient par l'application de la première partie du théorème 88.

Enfin, on peut réaliser la décomposition d'un nombre premier p dans le corps

$c(Z)$ en s'appuyant sur le théorème 88 et les propriétés des corps de décomposition et d'inertie.

On obtient ainsi le théorème :

THÉORÈME 125. — p étant un nombre premier non diviseur de $m = l_1^{h_1} l_2^{h_2} \ldots$, f le plus petit exposant positif pour lequel $p^f \equiv 1$, mod m, si l'on pose $\Phi(m) = ef$, p se décompose dans $c(Z)$ en

$$p = \mathfrak{P}_1 \ldots \mathfrak{P}_e,$$

$\mathfrak{P}_1, \ldots, \mathfrak{P}_e$ étant des idéaux premiers distincts de degré f de $c(Z)$.

Si l'on pose $m^* = p^h m$, on a dans le corps $c(Z^*)$ des $m^{*\text{ièmes}}$ racines de l'unité la décomposition

$$p = (\mathfrak{P}_1^* \ldots \mathfrak{P}_e^*)^{p^{h-1}(p-1)},$$

$\mathfrak{P}_1^*, \ldots, \mathfrak{P}_e^*$ étant des idéaux premiers distincts de degré f de $c(Z^*)$. [Kummer[15], Dedekind[5], Weber[4].]

Démonstration. — Supposons, pour abréger, $m = l_1^{h_1} l_2^{h_2}$, et désignons alors par $c^{(1)}$, $c^{(2)}$ les corps circulaires des racines $l_1^{h_1}$, $l_2^{h_2}$ ièmes de l'unité.

Soit p un nombre premier distinct de l_1, l_2 et soient $\mathfrak{p}^{(1)}$, $\mathfrak{p}^{(2)}$ deux facteurs premiers idéaux de p dans $c^{(1)}$ et $c^{(2)}$ respectivement; nous désignerons les corps de décomposition de $\mathfrak{p}^{(1)}$ dans $c^{(1)}$ et de $\mathfrak{p}^{(2)}$ dans $c^{(2)}$ par $c_d^{(1)}$, $c_d^{(2)}$. Soient f_1, f_2 les plus petits exposants pour lesquels $p^{f_1} \equiv 1 \bmod l_1^{h_1}$, $p^{f_2} \equiv 1 \bmod l_2^{h_2}$, et posons

$$l_1^{h_1-1}(l_1 - 1) = e_1 f_1 \qquad l_2^{h_2-1}(l_2 - 1) = e_2 f_2;$$

alors e_1, e_2 sont les degrés des corps $c_d^{(1)}$, $c_d^{(2)}$ et f_1, f_2 les degrés relatifs de $c^{(1)}$ par rapport à $c_d^{(1)}$ et de $c^{(2)}$ par rapport à $c_d^{(2)}$. D'après le théorème 88, le nombre premier p se décompose en $e_1 e_2$ idéaux dans le corps $c_d^{(1,2)}$ composé de $c_d^{(1)}$ et $c_d^{(2)}$; ces idéaux sont donc tous premiers du premier degré dans $c_d^{(1,2)}$. Nous considérons en particulier l'idéal premier $\mathfrak{p} = (\mathfrak{p}^{(1)}, \mathfrak{p}^{(2)})$ et nous désignons par $\mathfrak{P}$ un facteur premier de $\mathfrak{p}$ dans le corps c composé de $c^{(1)}$ et $c^{(2)}$; soit c_d le corps de décomposition de l'idéal premier $\mathfrak{P}$ dans c. Il résulte d'abord de la définition d'un corps de décomposition que $c_d^{(1,2)}$ doit, ou bien coïncider avec c_d, ou en faire partie comme sous-corps. Le groupe relatif du corps composé de $c^{(1)}$, $c_d^{(2)}$ par rapport à $c_d^{(1,2)}$ est cyclique de degré f_1; le groupe relatif du corps composé de $c_d^{(1)}$, $c^{(2)}$ par rapport à $c_d^{(1,2)}$ est cyclique de degré f_2. Nous en concluons que, f étant le plus petit commun multiple de f_1 et f_2, le groupe relatif de c par rapport à $c_d^{(1,2)}$ ne peut contenir aucun sous-groupe cyclique de degré supérieur à f. Comme c, corps d'inertie de l'idéal premier $\mathfrak{P}$, doit avoir un groupe relatif cyclique par rapport à c_d et que c_d contient $c_d^{(1,2)}$, il en résulte que ce groupe relatif cyclique de c par rapport à c_d est au plus de degré f.

D'autre part, faisons les remarques suivantes. Les deux corps $c^{(1)}$ et c_d ont comme sous-corps commun le corps $c_d^{(1)}$, mais aucun autre de degré supérieur, car autrement

$\mathfrak{p}^{(1)}$ devrait encore être décomposable dans $c^{(1)}$. De même les deux corps $c^{(2)}$ et c_d ont $c_d^{(2)}$ pour plus grand sous-corps commun. Prenons alors $c_d^{(1,2)}$ pour domaine de rationalité : c_d est alors un corps relatif par rapport à $c_d^{(1,2)}$, qui n'a ni avec $c^{(1)}$, ni avec $c^{(2)}$, aucun sous-corps commun relatif par rapport à $c_d^{(1,2)}$.

Nous en concluons facilement que c_d ne peut avoir un degré relatif par rapport à $c_d^{(1,2)}$ supérieur à $\frac{f_1 f_2}{f}$. Le corps c_d est donc au plus de degré $\frac{e_1 f_1 e_2 f_2}{f}$, c'est-à-dire que le groupe relatif de c par rapport à c_d est au moins de degré f. Ceci, joint au théorème démontré plus haut, montre que le degré du groupe relatif de c par rapport à c_d doit être égal à f, ce qui montre l'exactitude du théorème 125 dans notre cas particulier.

D'après le théorème 123, $Z = e^{\frac{2i\pi}{m}}$ satisfait à une équation irréductible $F(x) = 0$ de degré $\Phi(m)$ à coefficients entiers, et d'après la démonstration du théorème 87, cette équation $F(x) = 0$ reste même irréductible si l'on prend pour domaine de rationalité n'importe quel corps dont le discriminant soit premier à m. [Kronecker[3, 21].]

Voici comment on forme le polynome $F(x)$. Posons, pour abréger, $x^m - 1 = [m]$ et

$$\Pi_0 = [m],$$
$$\Pi_1 = \left[\frac{m}{l_1}\right]\left[\frac{m}{l_2}\right]\cdots,$$
$$\Pi_2 = \left[\frac{m}{l_1 l_2}\right]\left[\frac{m}{l_1 l_3}\right]\cdots\left[\frac{m}{l_2 l_3}\right]\cdots \qquad \text{etc.}$$

on a

$$F(x) = \frac{\Pi_0 \Pi_2 \Pi_4 \cdots}{\Pi_1 \Pi_3 \Pi_5 \cdots}.$$

[Dedekind[1], Bachmann[2].]

Si a est un entier rationnel et p un facteur premier de $F(x)$ premier à m, on voit que d'après le théorème 125 on a toujours $p \equiv 1 \bmod m$. Il y a par suite évidemment une infinité de nombres premiers vérifiant cette congruence.

§ 98. — Unités du corps $c\left(e^{\frac{2i\pi}{m}}\right)$. Définition des « unités circulaires ».

Théorème 126. — m étant une puissance du nombre premier l et g un nombre non divisible par l, l'expression

$$\frac{1 - Z^g}{1 - Z}$$

représente toujours une unité du corps $c\left(Z = e^{\frac{2i\pi}{m}}\right)$.

Si le nombre m contient plusieurs facteurs premiers et si g est premier à m, l'expression

$$1 - Z^g$$

représente toujours une unité dans le corps défini par $Z = e^{\frac{2i\pi}{m}}$.

Démonstration. — La première partie de ce théorème 126 a déjà été établie dans les démonstrations des théorèmes 117 et 120. Pour.démontrer la seconde, posons $m = l_1^{h_1} l_2^{h_2} l_3^{h_3} \dots$, et

$$\frac{g}{m} = \frac{a}{l_1^{h_1}} + \frac{b}{l_2^{h_2} l_3^{h_3} \dots},$$

où a est un entier premier à l_1 et b un entier premier à $l_2, l_3, \dots$. On a

(36) $$1 - Z^g = 1 - e^{\frac{2i\pi g}{m}} = 1 - e^{\frac{2i\pi a}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}.$$

Or, on a

$$\prod_{(x)} \left(1 - e^{\frac{2i\pi x}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}\right) = 1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \dots}},$$

le produit étant étendu à $x = 0, 1, 2, \dots, l_1^{h_1} - 1$, ou

(37) $$\prod_{(x')} \left(1 - e^{\frac{2i\pi x'}{l_1^{h_1}}} e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}\right) = \frac{1 - e^{\frac{2i\pi b l_1^{h_1}}{l_2^{h_2} l_3^{h_3} \dots}}}{1 - e^{\frac{2i\pi b}{l_2^{h_2} l_3^{h_3} \dots}}},$$

le produit étant étendu seulement à $x' = 1, 2, \dots, l_1^{h_1} - 1$.

Distinguons maintenant deux cas, suivant qu'il y a dans m deux facteurs premiers $l_1, l_2, \dots$, ou davantage : Dans le premier cas, le second membre de (37) est une unité d'après la première partie du théorème 126. Dans le second cas, nous pouvons admettre que le théorème 126 ait été démontré pour les corps $c\left(e^{\frac{2i\pi}{m^*}}\right)$, dont le nombre m^* a moins de facteurs premiers que m. Le théorème s'applique donc au corps formé des racines $\frac{m}{l_1^{h_1}}$ èmes de l'unité. Par suite, le numérateur et le dénominateur de la fraction du second nombre de (37) sont des unités. L'expression (36) est un facteur du produit du premier membre de (37), et, par conséquent, dans tous les cas, c'est une unité. C. q. f. d.

Une unité quelconque du corps circulaire $c\left(e^{\frac{2i\pi}{m}}\right)$ est le produit d'une racine de l'unité et d'une unité réelle. La racine de l'unité n'appartient pas toujours au corps $c\left(e^{\frac{2i\pi}{m}}\right)$, mais peut, si m contient plusieurs facteurs premiers différents, être, dans le cas de m pair, une racine $2m^{\text{ième}}$ de l'unité, et, dans le cas de m impair, une racine $4m^{\text{ième}}$. [Kronecker [7].] On a en particulier le théorème suivant déjà trouvé par Kummer.

Théorème 127. — *l* étant un nombre premier impair, si l'on considère, dans le corps $c(\zeta)$ défini par $\zeta = e^{\frac{2i\pi}{l}}$, le sous-corps $c(\zeta + \zeta^{-1})$ de degré $\frac{l-1}{2}$ défini par $\zeta + \zeta^{-1}$, un système quelconque d'unités fondamentales de ce corps réel $c(\zeta + \zeta^{-1})$ est en même temps système d'unités fondamentales de $c(\zeta)$.

Demonstration. — $\varepsilon(\zeta)$ étant une unité quelconque de $c(\zeta)$, $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ en est une autre, ayant ainsi que ses conjuguées pour valeur absolue 1, et c'est par suite, d'après le théorème 48, une racine de l'unité; posons $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta)^{-1}} = \pm \zeta^{2g}$ (1), où g est un entier. L'unité $\eta(\zeta) = \varepsilon(\zeta)\zeta^{-g}$ possède alors la propriété

$$(38) \qquad \frac{\eta(\zeta)}{\eta(\zeta^{-1})} = \pm 1.$$

Dans cette formule (38), le signe + est seul possible. Autrement $\eta(\zeta)$ serait une unité purement imaginaire; alors, posons $\eta^2 = \xi$, où ξ est une unité du sous-corps réel $c(\zeta + \zeta^{-1})$. La différente relative du nombre $\eta = \sqrt{2\xi}$ par rapport au sous-corps réel $c(\zeta + \zeta^{-1})$ est 2η, et, par suite, première à l. Par suite, la différente relative du corps $c(\zeta)$ par rapport à $c(\zeta + \zeta^{-1})$ devrait être première à l. Or, si $\mathfrak{l}^*$ désigne un facteur idéal premier quelconque de l dans le corps réel $c(\zeta + \zeta^{-1})$, cet idéal ne serait donc pas, d'après le théorème 93, égal au carré d'un idéal premier du corps $c(\zeta)$. Mais comme $\mathfrak{l}^*$ entre au plus à la puissance $\frac{l-1}{2}$ dans l, cette dernière conséquence serait contraire au théorème 117 sur la décomposition du nombre l dans $c(\zeta)$; donc, le second membre de (38) a bien le signe +. De $\eta(\zeta) = \eta(\zeta^{-1})$ suit que $\eta(\zeta)$ est réel. C. q. f. d.

Les unités données au théorème 126 sont imaginaires.

Pour en obtenir de réelles, formons, suivant que m est une puissance d'un nombre premier, ou contient plusieurs facteurs premiers différents, les expressions

$$\mathsf{E}_g = \sqrt{\frac{(1 - \mathsf{Z}^g)(1 - \mathsf{Z}^{-g})}{(1 - \mathsf{Z})(1 - \mathsf{Z}^{-1})}},$$

$$\mathsf{E}_g = \sqrt{(1 - \mathsf{Z}^g)(1 - \mathsf{Z}^{-g})},$$

où g est premier à m et où les $\sqrt{\ }$ sont pris avec le signe +. Ces unités s'appelleront simplement *unités circulaires*. Comme $1 - \mathsf{Z}^{-g} = -\mathsf{Z}^{-g}(1 - \mathsf{Z}^g)$, on reconnaît que, dans le premier cas, ces unités appartiennent au corps $c(\mathsf{Z})$ lui-même, tandis que, dans le second, ce sont des produits d'unités du corps $c(\mathsf{Z})$ par des racines $2m^{\text{ièmes}}$ ou $4m^{\text{ièmes}}$ de l'unité, suivant que m est pair ou impair.

(1) N. T. — On peut prendre un exposant pair, car on peut ajouter à l'exposant un multiple quelconque de l, qui est impair.

CHAPITRE XXIII.

Propriétés du corps circulaire comme corps abélien.

§ 99. — Le groupe du corps circulaire des racines $m^{\text{ièmes}}$ de l'unité.

Le corps circulaire des racines $m^{\text{ièmes}}$ de l'unité est toujours abélien et l'on a les théorèmes plus spéciaux ci-après.

Théorème 128. — l étant premier impair, le corps circulaire défini par $\mathsf{Z}=e^{\frac{2i\pi}{l^h}}$ est un corps cyclique.

Le corps circulaire défini par $\mathsf{Z}=e^{\frac{2i\pi}{2^h}}(h\geqslant 2)$ est composé du corps quadratique imaginaire $c(i)$ et du corps réel $c\left(e^{\frac{2i\pi}{2^h}}+e^{-\frac{2i\pi}{2^h}}\right)$. Ce corps réel est cyclique de degré 2^{h-2}.

Démonstration. — La première partie du théorème 128 résulte de l'introduction de la substitution $s=(\mathsf{Z}:\mathsf{Z}^r)$, où r est une racine primitive, mod l^h. Il est alors évident que toutes les substitutions du groupe de $c(\mathsf{Z})$ sont des puissances de s.

Pour démontrer la deuxième partie[1], considérons les substitutions :

$$s=(\mathsf{Z}:\mathsf{Z}^5),\qquad s'=(\mathsf{Z}:\mathsf{Z}^{-1})=(i:-i).$$

Il en résulte aisément que les puissances de s et leurs produits par s' représentent toutes les substitutions du corps $c(\mathsf{Z})$.

Le théorème 128 conduit immédiatement au groupe d'un corps circulaire des racines $m^{\text{ièmes}}$ de l'unité, m étant composé.

La détermination des corps de décomposition, d'inertie et de ramification pour un idéal premier donné de $c\left(e^{\frac{2i\pi}{m}}\right)$ peut se faire facilement avec l'aide des théorèmes démontrés paragraphes 95, 96 et 97, sur la décomposition d'un nombre premier dans un corps circulaire. On obtient ainsi en particulier ce résultat :

Théorème 129. — l étant premier impair, dans le corps circulaire $c(\mathsf{Z})$ des $l^{h\text{ièmes}}$ racines de l'unité, l'idéal premier $\mathfrak{L}=(1-\mathsf{Z})$ contenu dans l a pour corps de ramification le corps $c(\mathsf{Z})$ lui-même, et l'ensemble des nombres rationnels est à la fois corps de décomposition et corps d'inertie. $\mathfrak{P}$ étant un idéal premier de degré f de $c(\mathsf{Z})$, différent de $\mathfrak{L}$, $c(\mathsf{Z})$ est le corps d'inertie, et le corps de décomposition de $\mathfrak{P}$ est le sous-corps de degré $e=\frac{l^{h-1}(l-1)}{f}$ correspondant aux substitutions

$$s^f,\ s^{2f},\ \ldots,\ s^{ef},$$

s désignant une substitution $\mathsf{Z}:\mathsf{Z}^r$ dont les puissances engendrent complètement le groupe de $c(\mathsf{Z})$.

---

(1) N. T. — Il n'existe pas en effet de racines primitives, mod 2^{h+1}, pour $h\geqslant 2$.

§ 100. — Généralisation. — Théorème fondamental sur les corps abéliens.

Généralisons maintenant la notion de corps circulaire; désignons sous le nom de *corps circulaire* tout court non seulement tout corps $c\left(e^{\frac{2i\pi}{m}}\right)$ défini par des racines de l'unité d'indice m quelconque, mais aussi n'importe quel sous-corps du corps $c\left(e^{\frac{2i\pi}{m}}\right)$. Comme le corps $c\left(e^{\frac{2i\pi}{m}}\right)$ est toujours abélien, et que m et m' étant des exposants quelconques, le corps des racines $m^{\text{ièmes}}$ et celui des racines $m'^{\text{ièmes}}$ de l'unité sont tous les deux des sous-corps du corps des racines $m \, . \, m'^{\text{ièmes}}$, on a pour les corps circulaires plus généraux qu'on vient de définir les propositions suivantes :

Théorème 130. — Tout corps circulaire est abélien. Tout sous-corps d'un corps circulaire est un corps circulaire. Tout corps composé de corps circulaires est aussi circulaire :

Voici maintenant une proposition fondamentale qui fournit la réciproque de la première partie du théorème précédent.

Théorème 131. — *Tout corps abélien dans le domaine de rationalité des nombres rationnels est un corps circulaire.* [Kronecker[2, 13], Weber[1], Hilbert[5].]

Pour nous préparer à démontrer ce théorème fondamental, rappelons-nous que, d'après le théorème 48, tout corps abélien se compose de corps cycliques dont les degrés sont des nombres premiers ou des puissances de nombres premiers. Nous construisons alors les corps cycliques particuliers suivants. Soit u un nombre premier impair et u^h une de ses puissances d'exposant positif; alors le corps déterminé par $e^{\frac{2i\pi}{u^{h+1}}}$ est un corps cyclique de degré $u^h(u-1)$. Désignons par U_h le sous-corps cyclique de degré u^h de ce corps. Le nombre $e^{\frac{2i\pi}{2^{h+2}}} + e^{-\frac{2i\pi}{2^{h+2}}}$ détermine un corps cyclique réel de degré 2^h. Soit II_h ce dernier corps. Enfin, soit l^h une puissance d'un nombre premier quelconque l (égal à 2 ou non) et soit, en outre, p(¹) un nombre premier $\equiv 1$, mod l^h; alors le corps circulaire $c\left(e^{\frac{2i\pi}{p}}\right)$ de degré $p-1$ a évidemment un sous-corps cyclique de degré l^h. Soit P_h ce corps cyclique de degré l^h. Les corps U_h, II_h, P_h sont des corps circulaires de degrés u^h, 2^h, l^h; les discriminants de ces corps sont, vu les théorèmes 39 et 121, des puissances de u, de 2 et de p respectivement.

Nous montrerons dans les paragraphes suivants que tout corps abélien est un sous-corps d'un corps composé de $c(i)$ et de corps appropriés U_h, II_h, P_h. Il faut pour cela une série de considérations auxiliaires.

(¹) Voir la dernière remarque, § 97.

§ 101. — Lemme général sur les corps cycliques.

Lemme 15. — Si un corps cyclique C_h de degré l^h (l étant premier quelconque $= 2$ ou > 2) ne contient pas comme sous-corps le corps correspondant C_1 ou H_1, on obtient, en composant C_h avec le corps $c(\mathsf{Z})$ déterminé par $\mathsf{Z} = e^{\frac{2i\pi}{l^h}}$, un corps $c(\mathsf{Z}, C_h)$ de degré $l^{2h-1}(l-1)$, et il y a toujours dans $c(\mathsf{Z})$ un nombre κ ayant les propriétés suivantes : le corps $c(\mathsf{Z}, C_h)$ est aussi déterminé par les nombres Z et $\sqrt[l^h]{\kappa}$; si r est un entier quelconque non divisible par l, et $s = (\mathsf{Z} : \mathsf{Z}^r)$, la substitution correspondante du corps $c(\mathsf{Z})$, κ^{s-r} est la $l^{h\text{ième}}$ puissance d'un nombre de $c(\mathsf{Z})$.

Démonstration. — L'assertion relative au degré du corps $c(\mathsf{Z}, C_h)$ est une conséquence immédiate de ce que $c(\mathsf{Z})$ et C_h n'ont aucun sous-corps commun en dehors du corps des nombres rationnels. Soit alors α un nombre générateur du corps C_h, tel qu'aucune de ses puissances ne soit contenue dans un sous-corps de C_h; soit, de plus, t une substitution qui, avec ses puissances, engendre le groupe C_h. Posons, a et b étant des exposants quelconques,

$$K(\alpha^a, \mathsf{Z}^b) = \alpha^a + \mathsf{Z}^b . (t\alpha)^a + \mathsf{Z}^{2b} . (t^2\alpha)^2 + \ldots + \mathsf{Z}^{(l^h-1)b} . (t^{l^h-1}\alpha)^a.$$

Les expressions $K(\alpha, \mathsf{Z})$, $K(\alpha^2, \mathsf{Z})$, …, $K(\alpha^{l^h-1}, \mathsf{Z})$ ne peuvent s'annuler ensemble, car autrement, comme $K(\alpha^0, \mathsf{Z}) = 0$, le déterminant suivant

$$\begin{vmatrix} 1, & 1, & \ldots, & 1 \\ \alpha, & t\alpha, & \ldots, & t^{l^h-1}\alpha \\ \cdot & \cdot & \cdot & \cdot \\ \alpha^{l^h-1}, & (t\alpha)^{l^h-1}, & \ldots, & (t^{l^h-1}\alpha)^{l^h-1} \end{vmatrix}$$

devrait également s'annuler, et, vu la remarque du paragraphe 3, le nombre α ne serait pas un nombre générateur du corps C_h. Soit $\alpha^* = \alpha^a$ une puissance de α, pour laquelle $K = K(\alpha^*, \mathsf{Z})$, soit $\neq 0$. Comme $K(t\alpha^*, \mathsf{Z}^b) = \mathsf{Z}^{-b} K(\alpha^*, \mathsf{Z}^b)$, il en résulte que le nombre K^{l^h} et aussi tous les nombres $\dfrac{K(\alpha^*, \mathsf{Z}^b)}{K^b}$ sont des nombres du corps $c(\mathsf{Z})$. Comme on a

$$\alpha^* = \frac{1}{l^h} \{ K(\alpha^*, \mathsf{Z}) + K(\alpha^*, \mathsf{Z}^2) + \ldots + K(\alpha^*, \mathsf{Z}^{l^h}) \}$$

et que α^* est un nombre générateur du corps C_h, nous voyons que le corps défini par K et Z, de degré au plus égal à $l^{2h-1}(l-1)$, contient le corps $c(\mathsf{Z}, C_h)$ de degré $l^{2h-1}(l-1)$; le premier corps et le dernier sont donc identiques et le nombre $\kappa = K^{l^h}$ possède la propriété indiquée dans le lemme 15.

Faisons encore la remarque suivante. Le corps déterminé par Z et $\sqrt[l^h]{\kappa}$ est, on le voit aisément, cyclique relatif de degré relatif l^h vis-à-vis de $c(\mathsf{Z})$, et possède, par

suite, un seul sous-corps, qui contient $c(\mathsf{Z})$ et qui est cyclique relatif de degré l vis-à-vis de $c(\mathsf{Z})$. Si alors C_1 désigne le sous-corps de degré l de C_h, le corps formé de $c(\mathsf{Z})$ et C_1 doit être identique avec le corps formé de Z et $\sqrt[l]{\varkappa}$.

§ 102. SUR CERTAINS FACTEURS PREMIERS DU DISCRIMINANT D'UN CORPS CYCLIQUE DE DEGRÉ l^h.

LEMME 16. — Si C_h est un corps cyclique de degré l^h, l étant premier quelconque ($= 2$ ou $\neq 2$), et si C_1 est le sous-corps de degré l de C_h, les facteurs premiers p différents de l du discriminant de C_1 sont toujours $\equiv 1$, mod l^h.

Démonstration. — Considérons d'abord le cas où l est premier impair et où $h = 1$, et supposons que, contrairement au théorème, le discriminant de C_1 contienne un facteur premier $p \not\equiv 1 \bmod l$. Soit $\zeta = e^{\frac{2i\pi}{l}}$, r un nombre primitif mod l, et prenons dans le groupe du corps $c(\zeta)$ la substitution $s = (\zeta : \zeta^r)$. Si $\mathfrak{p}$ est un facteur idéal premier de p dans le corps $c(\zeta)$, il est, vu le théorème 119, comme $p \not\equiv 1 \bmod l$, d'un degré $f > 1$; donc, vu le théorème 129, le degré e du corps de décomposition de l'idéal premier $\mathfrak{p}$ est $< l - 1$; les autres facteurs premiers de p sont alors

$$\mathfrak{p}' = s\mathfrak{p}, \ \ldots, \ \mathfrak{p}^{(e-1)} = s^{e-1}\mathfrak{p},$$

tandis que $s^e\mathfrak{p} = \mathfrak{p}$, c'est-à-dire

(39) $$\mathfrak{p}^{s^e-1} = 1.$$

On a de même, pour les idéaux premiers conjugués de $\mathfrak{p}$: $\mathfrak{p}'$, $\mathfrak{p}''$, etc., les égalités correspondantes

(40) $$\mathfrak{p}'^{s^e-1} = 1, \quad \mathfrak{p}''^{s^e-1} = 1, \ldots$$

D'après le lemme 15, il y a dans $c(\zeta)$ un entier $\varkappa$, tel que les deux nombres ζ et $\sqrt[l]{\varkappa}$ engendrent le corps $c(\zeta, C_1)$ composé de $c(\zeta)$ et de C_1, et que $\varkappa^{s-r}$ est égal à la $l^{ième}$ puissance d'un nombre de $c(\zeta)$. Comme $s - r$ et $s^e - 1$ sont deux polynômes entiers à coefficients entiers en s, qui n'ont mod l aucun facteur commun, il existe trois polynômes entiers à coefficients entiers $\varphi(s)$, $\psi(s)$, $\chi(s)$, tels que

$$1 = (s^e - 1)\varphi(s) + (s - r)\psi(s) + l\chi(s),$$

et de là résulte

$$\varkappa = \varkappa^{(s^e-1)\varphi(s) + (s-r)\psi(s) + l\chi(s)} = \varkappa^{(s^e-1)\varphi(s)}\alpha^l,$$

où α est un nombre de $c(\zeta)$. Vu les égalités (39) et (40), $\varkappa^{s^e-1}$ est un nombre entier ou fractionnaire, tel que le numérateur et le dénominateur ne contiennent aucun facteur premier $\mathfrak{p}$, $\mathfrak{p}'$, ..., et sont, par suite, premiers à p; il en est donc de même de $\varkappa^{(s^e-1)\varphi(s)}$. Nous posons $\varkappa^{(s^e-1)\varphi(s)} = \frac{\gamma}{a^l}$, de façon que γ soit un entier de $c(\zeta)$ premier à p

et a un entier rationnel. Le corps $c(\zeta, C_1)$ est alors aussi engendré par les deux nombres ζ et $\sqrt[l]{\rho}$. Le discriminant relatif du nombre $\sqrt[l]{\rho}$, par rapport à $c(\zeta)$, est $\pm l^l \rho^{l-1}$; et comme ρ est premier à p, le discriminant relatif de $c(\zeta, C_1)$, par rapport à $c(\zeta)$, est aussi premier à p. Comme, d'autre part, le discriminant de $c(\zeta)$ n'est pas non plus divisible par p, le discriminant de $c(\zeta, C_1)$ est, vu le théorème 39, premier à p, et par suite aussi (théorème 85) le discriminant du corps C_1, contrairement à notre hypothèse.

l étant encore impair, soit $h > 1$. Soit $Z = e^{\frac{2i\pi}{l^h}}$, r un nombre primitif mod l^h, et soit, dans le corps $c(Z)$, la substitution $s = (Z : Z^r)$. Soit p un facteur premier $\neq l$ du discriminant de C_1 et $\mathfrak{p}$ un facteur idéal premier de p dans $c(Z)$.

Si nous supposons $p \equiv 1$ mod l, mais $\not\equiv 1$ mod l^h, l'idéal premier $\mathfrak{p}$ appartient toujours au sous-corps $c(Z^l)$ du corps $c(Z)$, c'est-à-dire que

$$\mathfrak{p}^{s^{l^{h-2}(l-1)}-1} = 1,$$

et de même pour les conjugués

$$\mathfrak{p}'^{s^{l^{h-2}(l-1)}-1} = 1, \quad \mathfrak{p}''^{s^{l^{h-2}(l-1)}-1} = 1, \ \ldots$$

Comme r est nombre primitif mod l^h, $r^{l^{h-2}(l-1)} \not\equiv 1$ mod l^h, et on peut, par suite, déterminer trois polynômes à coefficients entiers $\varphi(s)$, $\psi(s)$, $\chi(s)$, tels que

$$l^{h-1} = (s^{l^{h-2}(l-1)} - 1)\varphi(s) + (s - r)\psi(s) + l^h \chi(s);$$

on en déduit, $\varkappa$ étant déterminé comme au lemme 15,

$$\varkappa^{l^{h-1}} = \varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)} \alpha^{l^h},$$

où α est un nombre de $c(Z)$. Vu les propriétés déjà démontrées des idéaux premiers $\mathfrak{p}$, $\mathfrak{p}'$, $\mathfrak{p}''$, ..., $\varkappa^{s^{l^{h-2}(l-1)}-1}$, et, par suite, $\varkappa^{(s^{l^{h-2}(l-1)}-1)\varphi(s)}$ sont des nombres dont le numérateur et le dénominateur sont premiers à p. Nous pouvons donc mettre le dernier nombre sous la forme $\frac{\rho}{a^{l^h}}$, de façon que ρ soit un entier de $c(Z)$ premier à p et a un entier rationnel. Alors $\sqrt[l]{\varkappa} = \frac{\alpha}{a}\sqrt[l^h]{\rho}$, d'où on tire $\rho = \sigma^{l^{h-1}}$, σ étant aussi dans $c(Z)$.

Comme le corps $c(Z, \sqrt[l]{\varkappa})$ est, ainsi qu'on l'a remarqué à la fin du paragraphe 101, identique au corps composé de $c(Z)$ et de C_1 et que le discriminant relatif du nombre $\sqrt[l]{\sigma}$ vis-à-vis de $c(Z)$ a la valeur $\pm l^l \sigma^{l-1}$ première à p, le discriminant relatif du corps $c(Z, C_1)$ vis-à-vis de $c(Z)$ est premier à p. D'autre part, le discriminant de $c(Z)$ n'est pas davantage divisible par p, et il en est donc de même du discriminant de $c(Z, C_1)$ et par suite aussi de celui du corps C_1. Mais ceci est contraire à notre hypothèse.

Pour le cas de $l = 2$, supposons d'abord $h = 2$ et appliquons alors le lemme 15 au corps cyclique C_2 du quatrième degré. Posons $Z = e^{\frac{i\pi}{2}} = i$ et considérons la substitution de $c(Z)$ $s' = (i, -i)$. Soit C_1 le sous-corps quadratique de C_2 et supposons

qu'il y ait dans le discriminant de C_1 un facteur premier p impair $\equiv -1$, mod 4. Vu la dernière propriété, p est indécomposable dans $c(i)$. Si le nombre $\varkappa$ du lemme 15 est divisible par p, posons $\rho = \varkappa^{s-1}$. Comme d'autre part, d'après le lemme 15, on doit avoir $\varkappa^{s-1} = \alpha^4$, α étant dans $c(i)$, il en résulte $\varkappa^2 = \rho^{-1}\alpha^4$, c'est-à-dire $\sqrt{\varkappa} = \alpha\sqrt{\rho^{-1}}$. Donc ρ est le carré d'un nombre de $c(i)$; nous pouvons poser $\rho = \frac{\tau^2}{a^4}$ de façon que τ soit un entier de $c(i)$ premier à p et a un entier rationnel. Comme le corps $c(i, C_1)$ coïncide avec $c(i, \sqrt{\tau})$ et que, d'autre part, le discriminant relatif du nombre $\sqrt{\tau}$ vis-à-vis de $c(i)$ est premier à p, le discriminant relatif du corps $c(i, C_1)$ vis-à-vis de $C(i)$ est aussi premier à p; d'où il suit que le discriminant de C_1 n'est pas divisible par p, contrairement à l'hypothèse.

Si, l étant égal à 2, h est > 2, posons $Z = e^{\frac{2i\pi}{2^h}}$. Supposons que le discriminant de C_1 contienne un facteur premier $p \equiv 1$ mod 4 et $\not\equiv 1$ mod 2^h, et soit $\mathfrak{p}$ un facteur premier idéal de p dans $c(Z)$; $\mathfrak{p}$ resterait invariant dans une substitution $s_*^{2^{h-3}}$, où s_* est soit $(Z : Z^5)$, soit $(Z : Z^{-5})$; on aurait donc $\mathfrak{p}^{s_*^{2^{h-3}}} = \mathfrak{p}$. Comme $(\pm 5)^{2^{h-3}} \not\equiv 1$ mod 2^h, on aurait, comme plus haut, une égalité de la forme

$$2^{h-1} = (s_*^{2^{h-3}} - 1)\varphi(s_*) + (s_* \mp 5)\psi(s_*) + 2^h\chi(s_*),$$

d'où l'on tirerait une conclusion contraire à l'hypothèse que p divise le discriminant de C_1.

Le lemme 16 est ainsi complètement démontré et l'on en déduit sans difficulté la nouvelle proposition

Lemme 17. — Soit C_h un corps cyclique de degré l^h (l premier $= 2$ ou > 2); soit C_1 le sous-corps du $l^{\text{ième}}$ degré de C_h; soit p un facteur premier différent de l du discriminant du corps C_1 : on peut toujours trouver un corps abélien $C'_{h'}$ de degré $l^{h'} \leqq l^h$ ayant les deux propriétés suivantes :

1° Le corps composé de $C'_{h'}$ et d'un certain corps circulaire contient C_h comme sous-corps;

2° Le discriminant du corps $C'_{h'}$ ne contient que des facteurs premiers du discriminant du corps C_1, sauf le facteur p.

Démonstration. — D'après le lemme 16, le nombre premier p est $\equiv 1$, mod l^h; construisons d'après le paragraphe 100 le corps circulaire cyclique P_h de degré l^h, dont le discriminant est une puissance de p, et formons le corps composé de C_h et P_h dont le degré est $l^{h+h'}$. Dans P_h, on a $p = \mathfrak{p}^{l^h}$, où $\mathfrak{p}$ est un idéal premier de P_h. Soit $\mathfrak{P}$ un idéal premier facteur de $\mathfrak{p}$ dans $c(C_h, P_h)$. Comme l'idéal premier $\mathfrak{P}$ ne divise pas le degré $l^{h-h'}$ du corps $c(C_h, P_h)$, ce corps est le corps de ramification de l'idéal premier $\mathfrak{P}$ et par suite, vu le théorème 81, il est relatif cyclique et de degré relatif au moins égal à l^h par rapport au corps d'inertie $C'_{h'}$ de l'idéal premier $\mathfrak{P}$.

Comme d'ailleurs il ne peut y avoir dans $c(C_h, P_h)$ de corps cycliques relatifs de degré supérieur à l^h, $c(C_h, P_h)$ est donc exactement de degré l^h par rapport à $C'_{h'}$. Donc, le corps $C'_{h'}$ est de degré $l^{h'}$. La différente du corps d'inertie $C'_{h'}$ n'est pas divisible par $\mathfrak{P}$ (théorème 76) et par suite, eu égard au théorème 68, le discriminant du corps $C'_{h'}$ n'est pas divisible par p. D'un autre côté, ce discriminant n'a d'autres facteurs premiers (théorème 39) que ceux qui divisent le discriminant de C_h. Enfin, il résulte du théorème 87 que le corps composé de $C'_{h'}$ et P_h coïncide avec $c(C_h, P_h)$. Le corps C'_h possède donc les propriétés énoncées dans le lemme 17.

§ 103. — Le corps cyclique de degré u, dont le discriminant ne contient que u, et les corps cycliques de degré u^h et 2^h qui contiennent U_1 et H_1 comme sous-corps.

Lemme 18. — Si le discriminant d'un corps cyclique C_1 de degré premier impair u ne contient que u, C_1 coïncide avec U_1.

Démonstration. — Nous posons $\zeta = e^{\frac{2i\pi}{u}}$ et $s = (\zeta : \zeta^r)$, r étant racine primitive mod u ; $\lambda = 1 - \zeta$, et $\mathfrak{l} = (\lambda)$ idéal premier de $c(\zeta)$, $u = \mathfrak{l}^{u-1}$; enfin

$$s\lambda = 1 - \zeta^r \equiv r\lambda, \quad (\mathfrak{l}^2).$$

Puis considérons le nombre $\varkappa$ du lemme 15. Comme l'idéal premier $\mathfrak{l}$ de $c(\zeta)$ est du premier degré, il en résulte, si l'on pose $\rho = \varkappa^{(s-1)(u-1)}$, vu l'égalité $s\mathfrak{l} = \mathfrak{l}$ et le théorème 24, la congruence $\rho \equiv 1$, mod $\mathfrak{l}$. (Si l'on a dans un corps c un idéal $\mathfrak{j}$ et deux nombres fractionnaires α, β, la congruence $\alpha \equiv \beta$, mod $\mathfrak{j}$, doit s'entendre en ce sens qu'il y a dans c un nombre μ premier à $\mathfrak{j}$ pour lequel $\mu\alpha$, $\mu\beta$ sont des entiers de c tels que $\mu\alpha \equiv \mu\beta$, mod $(\mathfrak{j})$). Comme $r - 1$ est premier à u, le corps composé de C_1 et $c(\zeta)$ sera aussi engendré par ζ et $\sqrt[u]{\rho}$. En posant $\rho \equiv 1 + a\lambda$, mod $\mathfrak{l}^2$, où a est un entier rationnel, on a $\sigma = \rho\zeta^a \equiv 1$, mod $\mathfrak{l}^2$.

Démontrons maintenant que l'on a $\sigma \equiv 1$, mod $\mathfrak{l}^u$. Pour cela, supposons que $\sigma \equiv 1 + a\lambda^e$, mod $\mathfrak{l}^{e+1}$, l'exposant e étant $< u$ et a un entier rationnel non divisible par u.

Nous remarquons que, d'après le théorème 15, ρ^{s-r}, et par suite aussi σ^{s-r}, est la $u^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$: soit $\sigma^{s-r} = \beta^u$. Cette égalité donne la congruence $1 + ar^e\lambda^e - ar\lambda^e \equiv \beta^u$, mod $\mathfrak{l}^{e+1}$. De là résulte d'abord $\beta \equiv 1$, mod $\mathfrak{l}$, et ensuite $\beta^u \equiv 1$, mod $\mathfrak{l}^u$. On aurait enfin $ar^e \equiv ar$, mod $\mathfrak{l}$, ce qui est impossible, puisque r doit être racine primitive, mod u, et que $e > 1$. Par conséquent, on a bien $\sigma \equiv 1$, mod $\mathfrak{l}^u$.

Posons maintenant $\sigma = \frac{\tau}{a^{u(u-1)}}$, τ étant un entier de $c(\zeta)$ et a un entier rationnel : alors on a $\tau \equiv 1$, mod $\mathfrak{l}^u$. Si nous supposons alors le corps C_1 distinct du corps U_1, on

obtient en composant les corps $c(\zeta)$, U_1 et C_1 le corps $c(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ de degré $u(u-1)$. D'autre part, $\xi = \frac{1 - \sqrt[u]{\tau}}{\lambda}$ est, comme le montre l'équation $\frac{(\lambda\xi - 1)^u + \tau}{\lambda^u} = 0$, un entier du corps $c(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$, et le discriminant relatif de ce nombre vis à-vis de $c(\sqrt[u]{\zeta})$ est égal à $\varepsilon\tau^{u-1}$, ε étant une unité. Comme τ est premier à u, le discriminant relatif du corps $c(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$ vis-à-vis du corps $c(\sqrt[u]{\zeta})$ est aussi premier à u. Désignons donc par $\mathfrak{L}$ un facteur premier idéal de $\mathfrak{l}$ dans le corps $c(\sqrt[u]{\zeta}, \sqrt[u]{\tau})$; vu le théorème 93, $\mathfrak{L}$ aura dans ce corps un corps d'inertie I qui sera de degré u. Le discriminant de ce corps d'inertie I est premier à u et, vu le théorème 85, devrait alors avoir la valeur $+1$ ou -1. Mais il n'y a pas de corps cyclique de degré premier u et de discriminant ± 1 ; cela résulte soit immédiatement du théorème 44, soit du théorème 94, en prenant pour le corps c de ce théorème le corps des nombres rationnels, corps dans lequel tous les idéaux sont des idéaux principaux. Le lemme 18 est donc démontré.

Lemme 19. — Si un corps cyclique C_h de degré l^h, où l est un nombre premier impair ou est égal à 2, contient le corps U_1 ou le corps II_1 comme sous-corps, C_h est un sous-corps d'un corps composé de U_h ou de II_h avec un corps cyclique $C'_{h'}$ de degré $l^{h'} < l^h$.

Démonstration. — Soit $C_h \neq U_h$ ou II_h. Soit L_{h^*} le plus grand sous-corps contenu dans C_h en même temps que dans U_h ou dans II_h ; soit l^{h^*} le degré de L_{h^*}, h^* étant un nombre positif $< h$. Soit t une substitution qui, jointe à ses puissances, engendre le groupe du corps C_h, et z une substitution engendrant de même le corps U_h ou le corps II_h. Si nous posons $t^* = t^{l^{h^*}}$ et $z^* = z^{l^{h^*}}$, t^* et z^* engendrent les sous-groupes de degré l^{h-h^*} auxquels L_{h^*} appartient comme sous-corps, d'une part de C_h, d'autre part de U_h ou de II_h. Le corps C composé de C_h et de U_h ou II_h a, vis-à-vis de L_{h^*}, un degré relatif l^{2h-2h^*} et a donc un degré principal l^{2h-h^*}.

Pour obtenir le groupe G du corps C, désignons par ϑ un nombre générateur de C_h et par γ un nombre générateur du corps U_h ou II_h, et soient x, y des paramètres indéterminés. L'expression $\Theta = x\vartheta + y\gamma$ vérifie une équation de degré l^{2h-h^*}, dont les coefficients sont des polynômes à coefficients entiers en x, y, et qui est irréductible dans le domaine de rationalité de ces paramètres. Les diverses racines de cette équation sont de la forme

$$\Theta_{mn} = x t^m \vartheta + y z^n \gamma.$$

Comme, d'après un théorème connu, ϑ ainsi que γ s'expriment rationnellement en Θ avec des coefficients polynômes à coefficients entiers en x, y, il en est de même des racines Θ_{mn} ; nous posons donc

$$\Theta_{mn} = x t^m \vartheta + y z^n \gamma = \Phi_{mn}(\Theta),$$

Φ étant une telle fonction rationnelle. Soit maintenant A un nombre quelconque de C ou une fonction rationnelle de x, y à coefficients dans C; alors A est égal à une fonction rationnelle $F(\Theta)$ à coefficients polynômes entiers en x, y. Les conjugués de A s'expriment ainsi :

$$S_{mn}A = F\big(\Phi_{mn}(\Theta)\big),$$

et le système des l^{2h-h^*} substitutions correspondantes S_{mn} formera le groupe G du corps C. Vu

$$S_{mn}\Theta = xS_{mn}\zeta + yS_{mn}\gamma = xt^m\zeta + yz^n\gamma,$$

on a

$$S_{mn}\zeta = t^m\zeta, \qquad S_{mn}\gamma = z^n\gamma,$$

d'où résulte

$$(41) \qquad S_{mn}S_{m'n'} = S_{m+m',\, n+n'},$$

en convenant que l'on aura $S_{mn} = S_{m^*n^*}$, si $m \equiv m^*$ et $n \equiv n^*$, mod l^h. De (41) résulte que le groupe G est permutable, c'est-à-dire que le corps C est un corps abélien.

Soit r une racine primitive, mod l^h; comme $z^r\gamma$ est un des conjugués de γ, il doit y avoir une substitution de G pour laquelle n soit $\equiv r$, mod l^h. Soit $S_{mr} = s$ une telle substitution. Le degré du groupe cyclique engendré par s est l^h. On reconnaît aisément que toutes les substitutions du groupe G dont le second indice est $\equiv 0$ mod l^h forment un sous-groupe de degré l^{h-h^*}. Soit $s^* = S_{m^*0}$ une substitution génératrice de ce groupe cyclique. Le groupe G résulte alors évidemment de la composition des l^h puissances de s et des l^{h-h^*} puissances de s^*. Au sous-groupe des puissances de s^* correspond évidemment dans le corps C le sous-corps cyclique U_h ou Π_h. Au groupe engendré par s correspond dans C un certain sous-corps cyclique $C'_{h'}$ de degré l^{h-h^*}. Les deux corps U_h ou Π_h et $C'_{h'}$ n'ont pas de sous-corps commun en dehors du corps des nombres rationnels et le corps C résulte par suite de la composition de ces deux corps cycliques. Ce qui démontre le lemme 19.

§ 104. Démonstration du théorème fondamental sur les corps abéliens.

On a déjà montré (§ 48) que tout corps abélien est composé de corps cycliques dont les degrés sont des nombres premiers ou puissances de nombres premiers; il n'y a donc plus qu'à montrer que tout corps cyclique C_h de degré l^h, l étant premier, est un corps circulaire.

Pour le démontrer, supposons la proposition déjà établie pour les corps abéliens de degré $l^{h'} < l^h$.

Envisageons alors le sous-corps C_1 de degré l contenu dans C_h. Si nous supposons que le discriminant de C_1 contient un facteur premier p différent de l, le discrimi-

nant de C_h est aussi divisible par p (théorème 39). Il existe de plus (lemme 17) un corps abélien $C'_{h'}$ de degré $l^{h'} \leqq l^h$, tel que C_h est composé de $C'_{h'}$ et du corps circulaire P_h. Si donc $C'_{h'}$ est un corps cyclique de degré inférieur à l^h ou s'il est composé de plusieurs corps cycliques, $C'_{h'}$ est donc un corps circulaire, vu notre hypothèse, et il en est donc de même de C_h. Reste seulement à examiner le cas de $h' = h$, $C'_{h'} = C'_h$ étant alors un corps cyclique de degré l^h. Comme l'indique le même lemme 17, le discriminant de C_h' ne contient que des facteurs premiers du discriminant de C_h, mais non le facteur p; le discriminant de C_h' a donc au moins un facteur premier de moins que celui de C_h.

Désignons par C_1' le sous-corps de degré l de C_h'. Alors, si le discriminant de C_1 contient encore un facteur premier p' différent de l, nous pouvons faire pour le corps C_h' la même réduction que pour le corps C_h et nous arriverons, soit à conclure que C_h' est un corps circulaire, soit à un corps cyclique C_h'' de degré l^h, dont le discriminant contient un facteur premier de moins (p') que celui de C_h'. Après avoir appliqué m fois de suite le même procédé, ou bien nous arriverons à un corps $C_{h^{(m)}}^{(m)}$ qui sera circulaire, en vertu de notre hypothèse, ou à un corps cyclique $C_h^{(m)}$ de degré l^h, tel que le sous-corps $C_1^{(m)}$ de degré l contenu contenu dans $C_h^{(m)}$ aura un discriminant sans facteurs premiers ou n'ayant que le facteur l. Comme (voir lemme 18) un corps cyclique de degré l ne peut avoir un discriminant ± 1, c'est nécessairement le second cas qui se présente.

Distinguons alors le cas de l impair et celui de $l = 2$.

Dans le premier cas, $C_1^{(m)}$ coïncide avec U_1 (lemme 18). Dans le second cas $l = 2$, si $h = 1$ le corps $C_h^{(m)} = C_1^{(m)}$ est égal soit à $c(i)$, soit à $c(\sqrt{2}) = H_1$, c'est-à-dire est circulaire. Pour $h > 1$, on a encore $C_1^{(m)}$ égal à $c(\sqrt{2}) = H_1$. En effet, si $C_h^{(m)}$ est réel, $C_1^{(m)}$ l'est évidemment aussi, d'où la conclusion. Si $C_h^{(m)}$ est imaginaire, tous ses nombres réels forment un sous-corps réel de degré 2^{h-1}, et comme $C_1^{(m)}$ est nécessairement contenu dans ce corps réel, $C_1^{(m)}$ est encore réel et coïncide avec H_1.

Dans les deux cas ainsi séparés (en dehors de $l = 2$, $h = 1$), le corps $C_1^{(m)} = U_1$ ou H_1. D'après le lemme 19, $C_h^{(m)}$ est donc sous-corps d'un corps composé de U_h ou H_h et d'un corps cyclique C_{h^*} de degré $l^{h^*} < l^h$. Or, vu notre supposition, C_{h^*} est alors circulaire. Le théorème 131 est donc complètement démontré et l'on voit, de plus, le moyen de construire tous les corps abéliens de groupe et de discriminant donné.

CHAPITRE XXIV.

Les résolvantes d'un corps circulaire des racines $l^{\text{èmes}}$ de l'unité.

§ 105. — Définition et existence de la base normale.

Une base d'un corps abélien C sera dite *normale* lorsqu'elle se composera d'un entier N de C et de ses conjugués N′, N″, ..., $N^{(M-1)}$ (M étant le degré de C).

Lemme 20. — Si un corps abélien C possède une base normale, il en est de même de tout sous-corps *c* de C.

Démonstration. — M étant le degré de C, soient $t_1, \ldots, t_M$ les substitutions de ce corps abélien; soit N un entier de C formant avec ses conjugués une base normale de C. Si $t_1, \ldots, t_r$ forment alors le sous-groupe de ce groupe de M substitutions, auquel appartient le sous-corps *c* de C, on peut trouver $m = \frac{M}{r}$ substitutions $t'_1, \ldots, t'_m$ de la série $t_1, \ldots, t_M$ telles que ces M substitutions peuvent, à l'ordre près, se représenter par les produits

$$t'_1 t_1, \ldots, t'_1 t_r; \quad t'_2 t_1, \ldots, t'_2 t_r; \quad t'_m t_1, \ldots, t'_m t_r;$$

α étant un entier de *c* et par suite aussi de C, on a une égalité

$$\alpha = a_{11} t'_1 t_1 \mathsf{N} + \ldots + a_{1r} t'_1 t_r \mathsf{N} + \ldots + a_{m1} t'_m t_1 \mathsf{N} + \ldots + a_{mr} t'_m t_r \mathsf{N},$$

les a étant des entiers rationnels. Remarquons que les subtitutions $t_1, \ldots, t_r$ laissent α invariant, et que, d'autre part, il n'y a entre les $M = mr$ nombres $t'_1 t_1 \mathsf{N}, \ldots, t'_1 t_r \mathsf{N}, \ldots, t'_m t_r \mathsf{N}$ aucune relation linéaire à coefficients entiers non tous nuls; il en résulte évidemment

$$a_{11} = a_{12} = \ldots = a_{1r}; \ \ldots; \ a_{m1} = a_{m2} = \ldots = a_{mr};$$

donc, en posant

$$\nu = t_1 \mathsf{N} + t_2 \mathsf{N} + \ldots + t_r \mathsf{N},$$

les m nombres $t'_1 \nu, \ldots, t'_m \nu$ forment une base normale du corps c.

Théorème 132. — Tout corps abélien C de degré M, dont le discriminant D est premier à M, possède une base normale.

Démonstration. — Soient $p, p', \ldots,$ les facteurs premiers différents de D. Aucun d'eux ne divise M, et, par suite, vu la démonstration du théorème 131, le corps abé-

lien C est contenu comme sous-corps dans le corps engendré par les nombres $\zeta = e^{\frac{2i\pi}{p}}$, $\zeta' = e^{\frac{2i\pi}{p'}}$, etc., c'est-à-dire par $Z = e^{\frac{2i\pi}{pp'\ldots}}$. D'après le théorème 118, les nombres $1, \zeta, \ldots \zeta^{p-2}$ ou $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ forment une base de $c(\zeta)$; cette dernière est une base normale de ce corps. De même pour $c(\zeta')$, ...

Formons alors le système des $(p-1)(p'-1)\ldots$, nombres $\zeta^h\zeta'^{h'}$, où $h, h', \ldots$, prennent chacun toutes les valeurs $1, 2, \ldots, p-1$; $1, 2, \ldots, p'-1$; ... Ce système de $\Phi(pp'\ldots)$ nombres forme (théorème 88) une base de $c(Z)$, qui est évidemment normale. D'après le lemme 20, le corps abélien C a donc aussi une base normale. C. q. f. d.

§ 106. — Les corps abéliens de degré premier l et de discriminant p^{l-1}.

Les corps abéliens les plus simples et les plus importants avec les corps quadratiques sont ceux dont le degré est un nombre premier impair l et dont le discriminant d ne contient qu'un facteur premier p, ce dernier étant $\neq l$. Soit c un tel corps. D'après le lemme 16, on a nécessairement $p \equiv 1 \bmod l$. Le nombre premier p est dans c la $l^{\text{ième}}$ puissance d'un idéal premier du premier degré. D'après les remarques du théorème 79 et vu que c est toujours un corps réel, et que, par suite, d est positif, on a $d = p^{l-1}$.

Soient $1, t, t^2, \ldots, t^{l-1}$ les substitutions du groupe du corps c, et soit $\nu, t\nu, \ldots, t^{l-1}\nu$ une base normale de c. (Voir théorème 132.) Le nombre ν est alors toujours un nombre générateur du corps. Soit $\zeta = e^{\frac{2i\pi}{l}}$; l'expression

$$\Omega = \nu + \zeta . t\nu + \zeta^2 . t^2\nu + \ldots + \zeta^{l-1} . t^{l-1}\nu$$

s'appellera une *résolvante* (¹) du corps $c = c(\nu)$.

Une telle résolvante Ω est évidemment un entier du corps $c(\nu, \zeta)$ composé de $c(\nu)$ et $c(\zeta)$.

L'étude des bases normales et des résolvantes du corps abélien $c(\nu)$ conduit à des conséquences importantes relativement aux idéaux premiers facteurs de p dans $c(\zeta)$. Les développements de ce chapitre n'éprouvent que de légers changements, lorsqu'on prend le nombre 2 au lieu du nombre premier impair l.

(¹) N. T. — Nous croyons devoir traduire ainsi l'expression « Wurzel » ou « Wurzelzahl » employée par M. Hilbert; le mot résolvante est en effet le terme consacré depuis Lagrange. (*Réflexions sur la résolution algébrique des équations*, Mémoires de l'Académie de Berlin, 1770-1771.)

§ 107. — Propriétés caractéristiques des résolvantes.

Théorème 133. — Étant donné un corps abélien c de degré l et de discriminant $d = p^{l-1}$, l et p étant deux nombres premiers distincts, soit $\nu, t\nu, \dots, t^{l-1}\nu$ une base normale de ce corps. Si l'on pose $\zeta = e^{\frac{2i\pi}{l}}$, $\mathfrak{l} = (1 - \zeta)$, et $s = (\zeta : \zeta^r)$, r étant une racine primitive mod l, la résolvante Ω du corps $c(\nu)$, déduite de cette base normale, a les trois propriétés ci-après :

1° La $l^{\text{ième}}$ puissance de la résolvante $\omega = \Omega^l$ est un nombre du corps circulaire $c(\zeta)$, et, de plus, ω^{s-r} est égal à la $l^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$.

2° On a les congruences

$$\Omega \equiv \pm 1, \ (\mathfrak{l}), \qquad \omega \equiv \pm 1, \ (\mathfrak{l}^l).$$

3° $n(\omega)$, norme de ω dans $c(\zeta)$, est égale à $p^{\frac{l(l-1)}{2}}$.

Démonstration. — Les nombres Ω^l et Ω^{s-r} sont des nombres de $c(\zeta, \nu)$ invariants par la substitution $(\nu : t\nu)$. Ils appartiennent donc à $c(\zeta)$, d'où la première propriété.

Comme $\nu, t\nu, \dots, t^{l-1}\nu$ forment une base du corps $c(\nu)$, on a en particulier

$$1 = a_0\nu + a_1 t\nu + \dots + a_{l-1} t^{l-1}\nu$$

avec des coefficients a entiers. En effectuant sur cette égalité la substitution t, on voit que $a_0 = a_1 = \dots = a_{l-1} = \pm 1$, car ces coefficients ne peuvent avoir d'autre commun diviseur que ± 1.

Donc, $\nu + t\nu + \dots + t^{l-1}\nu = \pm 1$. D'où

$$\Omega = \nu + \zeta . t\nu + \dots + \zeta^{l-1} . t^{l-1}\nu \equiv \nu + t\nu + \dots + t^{l-1}\nu \equiv \pm 1, \qquad (\mathfrak{l}).$$

Puis, comme $\omega \mp 1 = (\Omega \mp 1)(\zeta\Omega \mp 1) \dots (\zeta^{l-1}\Omega \mp 1)$, on trouve la deuxième propriété du nombre ω.

Enfin, en appliquant convenablement la règle de multiplication des déterminants, on a

$$\begin{vmatrix} \nu, & t\nu, & \dots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \dots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \dots, & \nu \end{vmatrix} = (\nu + t\nu + \dots + t^{l-1}\nu)\, n(\Omega) = \pm\, n(\Omega),$$

où

$$n(\Omega) = (\nu + \zeta . t\nu + \dots + \zeta^{l-1} . t^{l-1}\nu) \dots (\nu + \zeta^{l-1} . t\nu + \dots + \zeta^{(l-1)^2} . t^{l-1}\nu)$$

est la norme relative de Ω par rapport au corps $c(\zeta)$. Le carré du déterminant du

premier membre est égal au discriminant du corps $c(\nu)$, c'est-à-dire p^{l-1}, et, par suite,

$$n(\omega) = \left(n(\Omega)\right)^l = p^{l\left(\frac{l-1}{2}\right)}. \qquad \text{C. q. f. d.}$$

Les trois propriétés précédentes de Ω suffisent inversement à caractériser complètement une telle résolvante. On a en effet la proposition suivante.

Théorème 134. — Soit l un nombre premier impair et $\zeta = e^{\frac{2i\pi}{l}}$, et p un nombre premier $\equiv 1$ mod l; si ω est un nombre du corps circulaire $c(\zeta)$, non égal à la $l^{\text{ème}}$ puissance d'un nombre de ce corps, et possédant les trois propriétés du théorème 133, $\Omega = \sqrt[l]{\omega}$ est une résolvante du corps abélien de degré l et de discriminant p^{l-1}.

Démonstration. — Le nombre $\Omega = \sqrt[l]{\omega}$ détermine un corps galoisien relatif de degré relatif l par rapport au corps $c(\zeta)$. Soit t la substitution du groupe relatif, pour laquelle $t\Omega = \zeta^{-1}\Omega$. Vu la première propriété du nombre ω, qui s'exprime par la formule $s\omega = \omega^r\alpha^l$, où α est un nombre de $c(\zeta)$, le corps de degré $l(l-1)$, composé de ζ et de Ω, est un corps galoisien. Le nombre α vérifie l'égalité

$$\omega^{1-r^{l-1}} = \alpha^{l\frac{s^{l-1}-r^{l-1}}{s-r}};$$

nous en déduisons la nouvelle relation

$$\omega^{\frac{1-r^{l-1}}{l}} = \alpha^{\frac{s^{l-1}-r^{l-1}}{s-r}}.$$

Nous entendrons maintenant par t et s les substitutions déterminées du groupe de ce corps galoisien $c(\zeta, \Omega)$, qui, en plus des conditions déjà fixées, remplissent encore les suivantes $t\zeta = \zeta$ et $s\Omega = \Omega^r\alpha$. Ces deux substitutions s et t sont permutables, car on a

$$st\Omega = \zeta^{-r}\Omega^r\alpha = ts\Omega,$$

c'est-à-dire que le corps $c(\zeta, \Omega)$ est un corps abélien. Le sous-groupe de $c(\zeta, \Omega)$, composé des puissances de s, est de degré $l-1$. Le sous-corps de $c(\zeta, \Omega)$ correspondant à ce sous-groupe est par suite de degré l; c'est encore un corps abélien, que nous désignerons par c.

Démontrons d'abord que le discriminant de ce corps c est premier à l. Comme $\Omega \equiv \pm 1$, mod $\mathfrak{l} = (1-\zeta)$, le quotient $\dfrac{\Omega \mp 1}{1-\zeta}$ est un nombre entier. Comme $t\Omega = \zeta^{-1}\Omega$, la différente relative de cet entier par rapport au corps $c(\zeta)$ a la valeur $\varepsilon\Omega^{l-1}$, ε étant une unité, et, par suite, la différente relative du corps $c(\zeta, \Omega)$ par rapport au corps $c(\zeta)$ est première à l. Si $\mathfrak{L}$ est un idéal premier facteur de $\mathfrak{l}$ dans $c(\zeta, \Omega)$, il n'y entre, vu le théorème 93, qu'à la première puissance, c'est-à-dire que $l = \mathfrak{L}^{l-1}\mathfrak{M}$, où $\mathfrak{M}$ n'est plus divisible par $\mathfrak{L}$. De là résulte, vu les paragraphes 39

et 40, que le corps d'inertie de l'idéal premier $\mathfrak{L}$ doit être de degré l, et que, par suite, c est lui-même ce corps d'inertie. D'après le théorème 76, la différente du corps c n'est pas divisible par $\mathfrak{l}$, et, par suite (théorème 68), le discriminant de c ne l'est pas non plus.

Nous posons

$$(41) \qquad \nu = \frac{\pm 1 + \Omega + s\Omega + s^2\Omega + \ldots + s^{l-2}\Omega}{l},$$

où le signe de 1 est le même que dans les congruences $\Omega \equiv \pm 1$, $s\Omega \equiv \pm 1$, ..., mod $\mathfrak{l}$; le numérateur de cette expression (41) à forme fractionnaire est donc $\equiv 0$, mod $\mathfrak{l}$. Ce numérateur représente un nombre de c. Si l est idéal premier dans c, ce numérateur doit donc être divisible par l et ν est un entier de c. Sinon, comme le discriminant de c ne contient pas le facteur l, on a dans ce corps une décomposition $l = \mathfrak{l}_1 \ldots \mathfrak{l}_l$ de l en l idéaux premiers distincts, et on a alors dans $c(\zeta, \Omega)$, comme le montre le théorème 88, la décomposition

$$\mathfrak{l} = (1 - \zeta) = (\mathfrak{l}, \mathfrak{l}_1)(\mathfrak{l}, \mathfrak{l}_2) \ldots (\mathfrak{l}, \mathfrak{l}_l).$$

Comme le numérateur de l'expression du second membre de (41) est divisible par l'idéal $(\mathfrak{l}, \mathfrak{l}_1)$, il est donc aussi, comme nombre entier de c, divisible par $\mathfrak{l}_1$. Il en résulte la divisibilité de ce numérateur par $\mathfrak{l}_2, \ldots, \mathfrak{l}_l$, et, par suite, finalement par l, de sorte que ν est encore un nombre entier du corps.

En se servant de la relation $t\Omega = \zeta^{-1}\Omega$, on tire de (41) les deux égalités

$$\begin{aligned} \nu + t\nu + t^2\nu + \ldots + t^{l-1}\nu &= \pm 1, \\ (42) \qquad \nu + \zeta . t\nu + \zeta^2 . t^2\nu + \ldots + \zeta^{l-1} . t^{l-1}\nu &= \Omega. \end{aligned}$$

En appliquant la règle de multiplication des déterminants (comme déjà dans la démonstration du théorème 133), on obtient ensuite

$$\mathsf{N} = \begin{vmatrix} \nu, & t\nu, & \ldots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \ldots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \ldots, & \nu \end{vmatrix} = \pm \Omega . s\Omega \ldots s^{l-2}\Omega,$$

d'où résulte, vu la troisième propriété de ω (théorème 133), la relation

$$\mathsf{N}^l = \pm p^{\frac{l(l-1)}{2}},$$

et, par conséquent,

$$\begin{vmatrix} \nu, & t\nu, & \ldots, & t^{l-1}\nu \\ t^{l-1}\nu, & \nu, & \ldots, & t^{l-2}\nu \\ \cdot & \cdot & \cdot & \cdot \\ t\nu, & t^2\nu, & \ldots, & \nu \end{vmatrix}^2 = p^{l-1}.$$

Nous démontrons ensuite que le discriminant du corps c est nécessairement égal à p^{l-1}. En effet, c'est, d'après la dernière relation, un diviseur positif de p^{l-1}. Comme ce ne peut être 1 (théorème 44 ou théorème 94), il contient donc le facteur p, et cela à la puissance $l-1$, d'après les remarques relatives au théorème 79. De la proposition ainsi démontrée, suit que ν, $t\nu$, ..., $t^{l-1}\nu$ forment une base, évidemment normale, du corps c. Et le nombre Ω est, vu (42), la résolvante du corps c déduite de cette base normale.

§ 108. — DÉCOMPOSITION DE LA $l^{\text{ième}}$ PUISSANCE D'UNE RÉSOLVANTE DANS LE CORPS DES RACINES $l^{\text{ièmes}}$ DE L'UNITÉ.

THÉORÈME 135. — l, p, ζ, r, s ayant leur signification précédente, $c(\nu)$ étant un corps abélien de degré l de discriminant $d = p^{l-1}$ et Ω une résolvante du corps $c(\nu)$, le nombre $\omega = \Omega^l$ a dans $c(\zeta)$ la décomposition

$$\omega = \mathfrak{p}^{l(1 + r_{-1}s + r_{-2}s^2 + \dots + r_{-l+2}s^{l-2})},$$

où $\mathfrak{p}$ est un idéal premier déterminé, facteur de p dans $c(\zeta)$, et où r_{-i} désigne le plus petit entier positif congru mod l à la puissance $-i^{\text{ième}}$ (r^{-i}) de la racine primitive r. [Kummer[6, 11].]

Démonstration. — Le nombre premier p se décompose dans $c(\zeta)$ en $l-1$ facteurs premiers idéaux distincts $\mathfrak{p}$, $s\mathfrak{p}$, ..., $s^{l-2}\mathfrak{p}$; le nombre ω doit être divisible par chacun d'eux. Car, d'après la démonstration du théorème 134, la différente relative du corps $c(\zeta, \Omega)$ par rapport au corps $c(\zeta)$ est un diviseur de $\Omega^l = \omega$; or, si ω était premier à $\mathfrak{p}$, la différente relative le serait aussi, ainsi que le discriminant de $c(\zeta, \Omega)$ (théorème 68), ce qui est impossible, puisqu'il est divisible par le discriminant de $c(\nu)$. A cause de $n(\omega) = p^{\frac{l(l-1)}{2}}$, $\mathfrak{p}$, $s\mathfrak{p}$, ..., $s^{l-2}\mathfrak{p}$ sont en même temps les seuls facteurs premiers idéaux de ω. Soit $\mathfrak{p}$ un de ces idéaux premiers dont l'exposant dans ω soit le plus petit possible; nous avons alors

$$\omega = \mathfrak{p}^{a_0 + a_1 s + \dots + a_{l-2} s^{l-2}},$$

a_0, ..., a_{l-2} étant des entiers positifs, dont aucun n'est inférieur à a_0. En formant $n(\omega)$ on obtient

$$a_0 + a_1 + \dots + a_{l-2} = \frac{l(l-1)}{2}.$$

Comme a_0, ..., a_{l-2} sont tous positifs, ces nombres ne peuvent donc tous être divisibles par l. A cause de la première propriété démontrée théorème 133, on a

$$\omega^{s-r} = \mathfrak{p}^{(s-r)(a_0 + a_1 s + \dots + a_{l-2} s^{l-2})} = \alpha^l.$$

où z est un nombre de $c(\zeta)$. Comme les idéaux premiers conjugués de $\mathfrak{p}$ en sont tous distincts et sont distincts entre eux, le polynôme en s

$$(s-r)(a_0 + a_1 s + \ldots + a_{l-2}s^{l-2}),$$

une fois développé, et s^{l-1} ayant été remplacé par 1, doit avoir tous ses coefficients divisibles par l, c'est-à-dire que ce polynôme est $\equiv a_{l-2}(s^{l-1}-1)$, mod l. Donc, a_{l-2} est $\not\equiv 0$, mod l, et si l'on pose $a_{l-2} \equiv r^{m-l+2}$, mod l, où m désigne l'un des nombres 0, 1, ..., $l-2$, on a pour $i = 0, 1, \ldots, l-2$ la congruence

$$a_i \equiv r^{m-i}, \quad (l).$$

Nous posons d'une façon générale

$$a_i = r_{m-i} + l b_i,$$

de façon que $0 < r_{m-i} < l$ et b_i étant un entier rationnel $\geqslant 0$. Comme

$$r_m + r_{m-1} + \ldots + r_{m-l+2} = 1 + 2 + \ldots + l - 1 = \frac{l(l-1)}{2},$$

on a $b_0 + b_1 + \ldots + b_{l-2} = 0$, et, par suite,

$$b_0 = 0, \quad b_1 = 0, \quad \ldots, \quad b_{l-2} = 0,$$

c'est-à-dire

$$a_i = r_{m-i}, \quad \text{pour} \quad i = 0, 1, \ldots, l-2.$$

Parmi les nombres $r_0, r_1, \ldots, r_{l-2}$, $r_0 = 1$ est évidemment le plus petit, et comme a_0 doit être le plus petit de $a_0, a_1, \ldots, a_{l-2}$, on a $a_0 = r_0 = 1$, c'est-à-dire $m = 0$, et alors $a_i = r_{-i}$. C. q. f. d.

§ 109. — Une équivalence relative aux idéaux premiers du premier degré du corps des racines $l^{\text{ièmes}}$ de l'unité.

Les développements précédents nous conduisent à une importante propriété des idéaux premiers facteurs d'un nombre premier $\equiv 1$, mod l, dans le corps des $l^{\text{ièmes}}$ racines de l'unité.

Théorème 136. — Soit l un nombre premier impair, $\zeta = e^{\frac{2i\pi}{l}}$, r un nombre positif racine primitive, mod l, $s = (\zeta : \zeta^r)$, $\mathfrak{p}$ étant alors un idéal premier du premier degré quelconque du corps circulaire $c(\zeta)$, on a l'équivalence

$$\mathfrak{p}^{q_0 + q_{-1}s + q_{-2}s^2 + \ldots + q_{-l+2}s^{l-2}} \sim 1,$$

où les quantités q_{-i} sont les entiers non négatifs définis par les égalités

$$q_{-i} = \frac{r r_{-i} - r_{-i-1}}{l} \qquad (i = 0, 1, \ldots, l-2).$$

$r_0, r_{-1}, \ldots, r_{-l+2}$ ont le même sens qu'au théorème 135 et, de plus, $r_1 = r_{-l+2}$.
[Kummer[11].]

Démonstration. — Donnons à p et à ω le même sens que dans le théorème 133 ; ω^{s-r} est alors la $l^{\text{ème}}$ puissance d'un nombre α dans $c(\zeta)$. En remplaçant ω par son expression en fonction de $\mathfrak{p}$ donnée au théorème 135, on a

$$\mathfrak{p}^{(s-r)(r_0+r_{-1}\cdot s+\cdots+r_{-l+2}\cdot s^{l-2})} = \alpha^l,$$

et cette égalité montre l'exactitude du théorème 136, si nous en tirons la décomposition de α.

C étant une classe quelconque d'idéaux du corps $c(\zeta)$ et $\mathfrak{j}$ un idéal de C, si l'on désigne par sC, s^2C, ..., $s^{l-2}C$ les classes déterminées par $s\mathfrak{j}$, $s^2\mathfrak{j}$, ..., $s^{l-2}\mathfrak{j}$, on tire du théorème 136 et du théorème 89 la relation

$$C^{q_0}(sC)^{q_{-1}}(s^2C)^{q_{-2}}\ldots(s^{l-2}C)^{q_{-l+2}} \sim 1.$$

§ 110. — Détermination de toutes les bases normales et de toutes les résolvantes.

Les théorèmes 133, 134, 135 permettent maintenant de déterminer toutes les résolvantes du corps abélien $c(\nu)$.

Théorème 137. — Ω et Ω^* désignant deux résolvantes distinctes du corps abélien c de degré premier l et de discriminant p^{l-1}, mais déduites de la même substitution génératrice t du groupe de ce corps, on a toujours $\Omega^* = \varepsilon\Omega$, ε étant une unité du corps $c(\zeta)$ vérifiant la congruence $\varepsilon \equiv \pm 1$, mod $\mathfrak{l} = (1-\zeta)$. Réciproquement, si ε est une telle unité dans $c(\zeta)$ et Ω une résolvante quelconque de c, $\Omega^* = \varepsilon\Omega$ est encore une résolvante de ce corps abélien c.

Démonstration. — Vu les hypothèses de la première partie, le quotient $\varepsilon = \frac{\Omega^*}{\Omega}$ est un nombre du corps composé de c et de $c(\zeta)$, qui reste invariant dans le changement de ζ, ν en ζ, $t\nu$ et qui appartient par suite au corps $c(\zeta)$. Prenons pour $\omega = \Omega^l$ l'expression donnée au théorème 135. Si alors $s^{-a}\mathfrak{p}$, a étant un des nombres 0, 1, 2, ..., $l-2$, est celui des $l-1$ idéaux premiers conjugués facteurs de p dans $c(\zeta)$ qui n'entre qu'à la première puissance dans $\omega^* = \Omega^{*l}$, on a évidemment, d'après le théorème 135,

$$\omega^* = \mathfrak{p}^{s^{-a}(r_0+r_{-1}\cdot s+\cdots+r_{-l+2}\cdot s^{l-2})},$$

et il en résulte que l'idéal premier $\mathfrak{p}$ entre dans ω^* exactement à la puissance r_{-a}. Le quotient $\frac{\omega^*}{\omega}$ peut donc se mettre sous la forme d'une fraction dont le numérateur contient l'idéal premier $\mathfrak{p}$ à la puissance $(r_{-a} - r_0)$, tandis que le dénominateur est premier à $\mathfrak{p}$. Comme, vu $\frac{\omega^*}{\omega} = \varepsilon^l$, l'exposant $r_{-a} - r_0$ doit être divisible par l, il en

résulte $r'_{u} = r_{u}$, c'est-à-dire $a = 0$. Par suite, ω^* et ω contiennent les mêmes puissances d'idéaux premiers et ε est donc une unité.

Le reste du théorème 137 ressort immédiatement des théorèmes 133 et 134.

Des résolvantes relatives à t, on déduit aisément, par la formule (41), toutes les bases normales $\nu, t\nu, \ldots, t^{l-1}\nu$ du corps abélien c.

§ 111. — La base normale et la résolvante de Lagrange.

Soit encore l un nombre premier impair, $\zeta = e^{\frac{2i\pi}{l}}$, et p un nombre premier de la forme $lm+1$; soit $\mathsf{Z} = e^{\frac{2i\pi}{p}}$ et soit R une racine primitive mod p. Enfin, soit c le corps abélien de degré l et de discriminant p^{l-1}.

Les $p-1$ nombres $\mathsf{Z}, \mathsf{Z}^2, \ldots, \mathsf{Z}^{p-1}$ forment une base normale du corps $c(\mathsf{Z})$: il résulte alors de la démonstration du lemme 20 que les nombres

$$\begin{aligned}
\lambda_0 &= \mathsf{Z} + \mathsf{Z}^{R^l} + \mathsf{Z}^{R^{2l}} + \ldots + \mathsf{Z}^{R^{(m-1)l}},\\
\lambda_1 &= \mathsf{Z}^{R} + \mathsf{Z}^{R^{1+l}} + \mathsf{Z}^{R^{1+2l}} + \ldots + \mathsf{Z}^{R^{1+(m-1)l}},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\lambda_{l-1} &= \mathsf{Z}^{R^{l-1}} + \mathsf{Z}^{R^{2l-1}} + \mathsf{Z}^{R^{3l-1}} + \ldots + \mathsf{Z}^{R^{ml-1}}
\end{aligned}$$

forment une base normale du corps c. On en déduit la résolvante suivante du même corps

$$\begin{aligned}
\Lambda &= \lambda_0 + \zeta\lambda_1 + \zeta^2\lambda_2 + \ldots + \zeta^{l-1}\lambda_{l-1},\\
&= \mathsf{Z} + \zeta\mathsf{Z}^{R} + \zeta^2\mathsf{Z}^{R^2} + \ldots + \zeta^{p-2}\mathsf{Z}^{R^{p-2}}.
\end{aligned}$$

Cette base normale particulière $\lambda_0, \lambda_1, \ldots, \lambda_{l-1}$ s'appellera *base normale de Lagrange* et la résolvante particulière Λ la *résolvante de Lagrange*.

§ 112. — Propriétés caractéristiques de la résolvante de Lagrange.

La résolvante de Lagrange Λ du corps c se distingue des autres résolvantes de c par les propriétés suivantes :

Théorème 138. — Si l'on représente la $l^{\text{ème}}$ puissance Λ^l de la résolvante de Lagrange, d'après le théorème 135, par la formule

$$\Lambda^l = \mathfrak{p}^{\ldots}$$ [illegible]

$\mathfrak{p}$ est l'idéal premier défini par la formule

$$\mathfrak{p} = (p, \zeta - R^m), \left(m = \frac{p-1}{l}\right).$$

les lettres ayant, du reste, le même sens qu'au théorème 135. La résolvante de Lagrange Λ est $\equiv -1 \bmod \mathfrak{l}$ et de plus sa valeur absolue est égale à $\sqrt{p}$. Réciproquement, si une résolvante Ω a les propriétés précédentes et que de plus Ω^l contienne l'idéal premier $\mathfrak{p}$ exactement à la première puissance, on a $\Omega = \zeta^* \Lambda$, où ζ^* est une racine $l^{\text{ème}}$ de l'unité.

Démonstration. — En posant $\mathfrak{P} = (1-Z, \mathfrak{p})$, on voit, à l'aide de $(1-Z)^{p-1} = p$ et $(p, \mathfrak{p}^{p-1}) = \mathfrak{p}$, que

$$\mathfrak{P}^{p-1} = \left(p, (1-Z)^{p-2}\mathfrak{p}, \ldots, \mathfrak{p}^{p-1}\right) = \mathfrak{p};$$

il est alors visible que $\mathfrak{P}$ est idéal premier dans le corps défini par ζ et Z et que le nombre $1 - Z$ ne contient cet idéal premier qu'à la première puissance.

Posons $Z = 1 + H$ et tenons compte de la congruence $\zeta \equiv R^{-m}$, mod $\mathfrak{p}$, et de l'égalité $(1+H)^p = 1$; on a

$$\Lambda \equiv \sum_{(x)} R^{-mx}(1+H)^{R^x}, \qquad (\mathfrak{p}),$$

$$\equiv \sum_{(X)} \left\{ X^{-m} \sum_{(Y)} \binom{X}{Y} H^Y \right\}, \quad (\mathfrak{p}),$$

où les sommes respectives doivent être étendues aux valeurs $x = 0, 1, 2, \ldots, p-2$; $X = 1, 2, \ldots, p-1$; $Y = 0, 1, 2, \ldots, X$. De la dernière formule on déduit, en changeant l'ordre des sommations :

(43) $$\Lambda \equiv -\frac{H^m}{m!}, \qquad (\mathfrak{P}^{m+1}).$$

La résolvante de Lagrange Λ contient donc exactement la $m^{\text{ème}}$ puissance de $\mathfrak{P}$ en facteur, et par suite Λ^l n'est divisible que par la première puissance de $\mathfrak{p}$.

Désignons par $\overline{\Lambda}$ le nombre imaginaire conjugué de Λ; on a

$$\overline{\Lambda} = Z^{-1} + \zeta^{-1} Z^{-R} + \zeta^{-2} Z^{-R^2} + \ldots + \zeta^{-p+2} Z^{-R^{p-2}},$$

et en groupant ensemble dans le produit $\Lambda\overline{\Lambda}$ les $p-1$ termes multipliés par une même puissance de ζ

$$\begin{aligned} \Lambda\overline{\Lambda} = {} & (1 + 1 + \ldots + 1) \\ & + \zeta\,(Z^{R-1} + Z^{R^2-R} + \ldots + Z^{R^{p-1}-R^{p-2}}) \\ & \cdots\cdots\cdots\cdots\cdots\cdots \\ & + \zeta^{p-2}(Z^{R^{p-2}-1} + Z^{R^{p-1}-R} + \ldots + Z^{R^{2p-4}-R^{p-2}}) \\ = {} & p - 1 - (\zeta + \zeta^2 + \ldots + \zeta^{p-2}) = p. \end{aligned}$$

La première partie du théorème est ainsi démontrée.

La seconde partie en est précisément la réciproque. Son exactitude découle aisément des théorèmes 135 et 137, avec l'aide du théorème 48; on doit pour cela remarquer que, si un nombre d'un corps abélien a la valeur absolue 1, il en est de même de ses conjugués.

Nous pouvons obtenir, d'une façon analogue à (43), les congruences suivantes [Jacobi [2]] :

(44) $$s^{-i}\Lambda \equiv -\frac{\Pi^{r_{-i}m}}{(r_{-i}m)!}, \qquad (\mathfrak{P}^{r_{-i}m+1})$$

pour $i = 0, 1, 2, \ldots, l-2$. En nous rappelant que $\Lambda \equiv -1 \bmod \mathfrak{l}$ et que $|\Lambda| = \sqrt{p}$, nous tirons de ces congruences (44) une autre démonstration des théorèmes 135 et 136. [Kummer [6, 11].]

Tous les théorèmes de ce chapitre XXIV s'appliquent aussi au cas de $l = 2$, sauf que le discriminant du corps abélien c prend la valeur $d = (-1)^{\frac{p-1}{2}} p$.

La racine de Lagrange Λ du corps c est un entier du corps composé de $c(\zeta)$ et c, caractérisé au facteur ζ^* près par les propriétés énumérées par les théorèmes 133 et 138. Pour fixer enfin même ce facteur ζ^*, on devrait poser $\Lambda = \sqrt{p}e^{2i\pi\varphi}$, de façon que $0 \leqq \varphi < 1$, et ensuite voir dans lequel des l intervalles

$$0 \leqq \varphi < \frac{1}{l}, \quad \frac{1}{l} \leqq \varphi < \frac{2}{l}, \quad \ldots, \quad \frac{l-1}{l} \leqq \varphi < 1$$

le nombre φ est placé. Cette question soulève dans le cas particulier de $l = 2$ le célèbre problème de la détermination du signe des sommes de Gauss (voir § 124). Pour $l = 3$, nous sommes conduits à un problème traité par Kummer. [Kummer [2, 4].]

Les nombres de la base normale de Lagrange sont ordinairement appelés *périodes*. La bibliographie indique une série de travaux relatifs à ces périodes, ainsi qu'à des nombres entiers analogues de corps circulaires. [Kummer [3, 17], Fuchs [1, 2], Schwering [1, 3, 4], Kronecker [17], Smith [1].] On y trouve aussi des recherches sur des corps circulaires particuliers. [Berkenbusch [1], Eisenstein [10], Schwering [2], Weber [1, 2, 4], Wolfskehl [1].] Mentionnons aussi que, si le nombre premier l est < 100 et $\neq 29$ ou de 41, le corps circulaire $c(\zeta)$ contient toujours une classe d'idéaux dont les puissances fournissent toutes les classes du corps. [Kummer [11, 13].]

CHAPITRE XXV.

Loi de réciprocité pour les résidus de $l^{\text{ièmes}}$ puissances entre un nombre rationnel et un nombre du corps des racines $l^{\text{ièmes}}$ de l'unité.

§ 113. — Caractère de puissance d'un nombre et symbole $\left(\frac{\alpha}{\mathfrak{p}}\right)$.

Soit l un nombre premier impair, $\zeta = e^{\frac{2i\pi}{l}}$, et $c(\zeta)$ le corps circulaire engendré par ζ; p étant ensuite un nombre premier, autre que l, et $\mathfrak{p}$ un des idéaux premiers facteurs de p dans $c(\zeta)$, f étant son degré, on a, d'après le théorème 24, pour tout entier α du corps non divisible par $\mathfrak{p}$, la congruence

$$\alpha^{p^f-1} - 1 \equiv 0, \quad (\mathfrak{p}).$$

Comme $p^f - 1$ est divisible par l d'après le théorème 119, le premier membre de cette congruence s'écrit

$$\alpha^{p^f-1} - 1 = \prod_{(k)} \left(\alpha^{\frac{p^f-1}{l}} - \zeta^k\right),$$

où le produit est étendu aux valeurs $k = 0, 1, 2, \ldots, l-1$. Il en résulte que la congruence

$$\alpha^{\frac{p^f-1}{l}} \equiv \zeta^k, \quad (\mathfrak{p})$$

est vérifiée pour une valeur de k et une seule.

La racine de l'unité qui y figure, ζ^k, s'appelle *le caractère de puissance du nombre* α *par rapport à l'idéal premier* $\mathfrak{p}$ dans le corps $c(\zeta)$, et on représente cette racine de l'unité ζ^k par le *symbole*

$$\left(\frac{\alpha}{\mathfrak{p}}\right),$$

de sorte qu'on a la congruence

(45) $$\alpha^{\frac{p^f-1}{l}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right), \quad (\mathfrak{p}).$$

[Kummer].

α et β étant deux entiers de $c(\zeta)$ non divisibles par $\mathfrak{p}$, on a, on le voit facilement, l'égalité

$$\left\{\frac{\alpha\beta}{\mathfrak{p}}\right\}=\left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\beta}{\mathfrak{p}}\right\}.$$

Si le nombre entier α est en particulier congru mod $\mathfrak{p}$ à la $l^{\text{ème}}$ puissance d'un nombre entier de $c(\zeta)$, on dit que α est *résidu de puissance $l^{\text{ème}}$ de l'idéal premier* $\mathfrak{p}$. On a la proposition :

THÉORÈME 139. — $\mathfrak{p}$ étant un idéal premier différent de $\mathfrak{l}=(1-\zeta)$ et α un entier de $c(\zeta)$ premier à $\mathfrak{p}$, la condition nécessaire et suffisante pour que α soit résidu de puissance l^{eme} de $\mathfrak{p}$ est $\left\{\frac{\alpha}{\mathfrak{p}}\right\}=1$.

Démonstration. — Si $\alpha\equiv\beta^l$, mod $\mathfrak{p}$, β étant un nombre de $c(\zeta)$, on a $\alpha^{\frac{p^f-1}{l}}\equiv\beta^{p^f-1}\equiv 1$, c'est-à-dire $\left\{\frac{\alpha}{\mathfrak{p}}\right\}=1$. Pour démontrer la réciproque, désignons par ρ un nombre primitif mod $\mathfrak{p}$ et posons $\alpha\equiv\rho^h$, mod $\mathfrak{p}$. Si nous supposons que $\alpha^{\frac{p^f-1}{l}}=\rho^{\frac{h(p^f-1)}{l}}\equiv 1$, il en résulte $\frac{h(p^f-1)}{l}\equiv 0$, mod p^f-1, c'est-à-dire que h est divisible par l, et, par suite, α est un résidu de puissance $l^{\text{ème}}$, mod $\mathfrak{p}$, ce qu'il fallait démontrer.

Le caractère de puissance $\left\{\frac{\rho}{\mathfrak{p}}\right\}$ d'un nombre primitif, mod $\mathfrak{p}$, est certainement différent de 1. Car dans la série des puissances ρ, ρ^2, etc., ρ^{p^f-1} est la première qui soit $\equiv 1$, mod $\mathfrak{p}$, et, par suite, $\rho^{\frac{p^f-1}{l}}\not\equiv 1$, mod $\mathfrak{p}$.

Soit $\left\{\frac{\rho}{\mathfrak{p}}\right\}=\zeta^g$; déterminons un entier rationnel g^* premier à p^f-1, et tel que $gg^*\equiv 1$, mod l; alors $\rho^*=\rho^{g^*}$ est un nombre primitif, mod $\mathfrak{p}$, pour lequel $\left\{\frac{\rho^*}{\mathfrak{p}}\right\}=\zeta$. Si alors α est un entier de $c(\zeta)$ non divisible par $\mathfrak{p}$, et si l'on a $\alpha\equiv\rho^{*h}$, mod $\mathfrak{p}$, on a $\left\{\frac{\alpha}{\mathfrak{p}}\right\}=\zeta^h$.

On conclut aisément de là que le système complet des p^f-1 nombres incongrus mod $\mathfrak{p}$: $1, \rho^*, \rho^{*2}, \ldots, \rho^{*p^f-2}$, se décompose en l systèmes partiels, dont chacun renferme $\frac{p^f-1}{l}$ nombres ayant le même caractère de puissance. En particulier, il y a exactement $\frac{p^f-1}{l}$ résidus de puissance $l^{\text{ème}}$ incongrus mod $\mathfrak{p}$.

Si $\mathfrak{b}$ est un idéal quelconque de $c(\zeta)$ premier à $\mathfrak{l}$ et α un entier de ce corps premier à $\mathfrak{b}$, si l'on pose $\mathfrak{b}=\mathfrak{p}\mathfrak{q}\ldots\mathfrak{w}$, $\mathfrak{p}$, $\mathfrak{q}$, etc., étant des idéaux premiers, on définira le symbole $\left\{\frac{\alpha}{\mathfrak{b}}\right\}$ par l'égalité

$$\left\{\frac{\alpha}{\mathfrak{b}}\right\}=\left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\alpha}{\mathfrak{q}}\right\}\cdots\left\{\frac{\alpha}{\mathfrak{w}}\right\}.$$

§ 114. — Lemme sur le caractère de puissance de la $l^{\text{ième}}$ puissance de la résolvante de Lagrange.

Eisenstein est parvenu à découvrir et à démontrer cette loi de réciprocité qui existe entre un nombre entier rationnel et un nombre quelconque du corps $c(\zeta)$ ($\zeta = e^{\frac{2i\pi}{l}}$, l premier impair). Cette loi de réciprocité est en même temps un auxiliaire, jusqu'ici indispensable, pour la démonstration de la loi de réciprocité plus générale de Kummer. [Voir chap. XXXI.] Pour démontrer la loi de réciprocité d'Eisenstein, il faut d'abord le lemme suivant :

Lemme 21. — Soit $\zeta = e^{\frac{2i\pi}{l}}$; soit p un nombre premier de la forme $ml+1$, R un nombre primitif mod p, et $\mathfrak{p}$ l'idéal premier du premier degré de $c(\zeta)$:

$$\mathfrak{p} = (p,\ \zeta - \mathrm{R}^{-m});$$

posons $\mathsf{Z} = e^{\frac{2i\pi}{p}}$, la résolvante de Lagrange Λ :

$$\Lambda = \mathsf{Z} + \zeta \mathsf{Z}^{\mathrm{R}} + \zeta^2 \mathsf{Z}^{\mathrm{R}^2} + \ldots + \zeta^{p-2} \mathsf{Z}^{\mathrm{R}^{p-2}}$$

et $\pi = \Lambda^l$. Soit enfin q un nombre premier quelconque différent de l et p, $\mathfrak{q}$ un idéal premier facteur de q dans $c(\zeta)$ et de degré g ; alors le caractère de puissance du nombre $\pi = \Lambda^l$ par rapport à $\mathfrak{q}$ s'exprime par la formule

$$\left(\frac{\pi}{\mathfrak{q}}\right) = \left(\frac{q}{\mathfrak{p}}\right)^g.$$

Démonstration. — En élevant g fois à la $q^{\text{ième}}$ puissance, on a la congruence

(46) $$\Lambda^{q^g} \equiv \mathsf{Z}^{q^g} + \zeta^{q^g} \mathsf{Z}^{\mathrm{R}q^g} + \zeta^{2q^g} \mathsf{Z}^{\mathrm{R}^2 q^g} + \ldots + \zeta^{(p-2)q^g} \mathsf{Z}^{\mathrm{R}^{p-2} q^g}, \quad (q).$$

En remarquant que $q^g \equiv 1$, mod l, d'après le théorème 119, et en posant $q^g \equiv \mathrm{R}^h$, mod p, le second membre de (46) devient

$$\mathsf{Z}^{\mathrm{R}^h} + \zeta \mathsf{Z}^{\mathrm{R}^{h+1}} + \zeta^2 \mathsf{Z}^{\mathrm{R}^{h+2}} + \ldots + \zeta^{p-2} \mathsf{Z}^{\mathrm{R}^{h+p-2}} = \zeta^{-h} \Lambda.$$

D'où résulte, Λ étant premier à q, vu le théorème 138, la congruence

$$\Lambda^{q^g - 1} \equiv \zeta^{-h}, \quad (q),$$

et on a donc certainement

$$\Lambda^{q^g-1} = \pi^{\frac{q^g-1}{l}} \equiv \zeta^{-h}, \quad (\mathfrak{q}),$$

c'est-à-dire que

(47) $$\left(\frac{\pi}{\mathfrak{q}}\right) = \zeta^{-h}.$$

D'autre part, on tire des congruences $q^q \equiv \mathrm{R}^h$, mod p, et $\mathrm{R}^m \equiv \zeta^{-1}$, mod $\mathfrak{p}$, les relations

$$q^{\frac{q(p-1)}{l}} = q^{qm} \equiv \mathrm{R}^{hm} \equiv \zeta^{-h}, \quad (\mathfrak{p}),$$

c'est-à-dire

(48) $$\left\{\frac{q^q}{\mathfrak{p}}\right\} = \left(\frac{q}{\mathfrak{p}}\right)^q = \zeta^{-h}. \qquad \text{C. q. f. d.}$$

§ 115. — Démonstration de la loi de réciprocité entre un nombre rationnel et un nombre quelconque de $c(\zeta)$.

Soit $\mathfrak{l} = (1-\zeta)$ l'idéal premier de l dans le corps $c(\zeta)$. Appelons *semi-primaire* un entier α de $c(\zeta)$, premier à $\mathfrak{l}$ et congru mod $\mathfrak{l}^2$ à un entier rationnel. Un entier rationnel, non divisible par l, est, par suite, toujours semi-primaire. Tout entier α de $c(\zeta)$, non divisible par $\mathfrak{l}$, peut toujours être changé en un nombre semi-primaire lorsqu'on le multiplie par une puissance convenable de ζ. Si, en effet, on a

$$\alpha \equiv a + b(1-\zeta), \quad (\mathfrak{l}^2),$$

a et b étant des entiers rationnels, on a

$$\zeta^{b^*} \cdot \alpha \equiv a, \quad (\mathfrak{l}^2)$$

si l'on détermine b^* par la congruence (1) $ab^* \equiv b$, mod l. Le nombre $\zeta^{b^*}\alpha$ est par suite semi-primaire.

Cette remarque préliminaire faite, voici l'expression de la loi de réciprocité d'Eisenstein.

Théorème 140. — *a étant un nombre entier rationnel, non divisible par le nombre premier impair l, et α un entier semi-primaire quelconque premier à a du corps $c(\zeta)$ des racines $l^{\text{ièmes}}$ de l'unité, on a dans ce corps*

$$\left\{\frac{a}{\alpha}\right\} = \left\{\frac{\alpha}{a}\right\}.$$

[Eisenstein[2].]

---

(1) N. T. $ab^* \equiv b$ mod l et, par suite, mod $\mathfrak{l}^2$. On a en effet alors

$$\alpha\zeta^{b^*} \equiv a\zeta^{b^*} + b\zeta^{b^*}(1-\zeta) \equiv a[\zeta^{b^*} + b^*\zeta^{b^*}(1-\zeta)], \quad (\mathfrak{l}^2)$$
$$\equiv a[1 + \zeta^{b^*} - 1 + b^*\zeta^{b^*}(1-\zeta)] \equiv a + a(1-\zeta)(b^*\zeta^{b^*} - \zeta^{b^*-1} - \zeta^{b^*-2} \ldots - 1)$$
$$\equiv a + a(1-\zeta)(\zeta^{b^*} - \zeta^{b^*-1} + \zeta^{b^*} - \zeta^{b^*-2} + \ldots + \zeta^{b^*} - 1)$$
$$\equiv a, \quad \text{mod } \mathfrak{l}^2.$$

Démonstration. — Soit r une racine primitive mod l et $s = (\zeta : \zeta^r)$. Supposons d'abord que a soit un nombre premier q et que α ne contienne que des idéaux premiers du premier degré. Soit $\mathfrak{q}$ un facteur idéal premier quelconque, de degré g, de q dans $c(\zeta)$, soit p un facteur premier de la norme $n(\alpha)$, et donnons à $\mathfrak{p}$ et à π le même sens que dans le lemme 21, s^u étant alors une puissance quelconque de s, l'application du lemme 21 aux idéaux premiers $s^{-u}\mathfrak{q}$ et $\mathfrak{p}$ donne

$$\left(\frac{\pi}{s^{-u}\mathfrak{q}}\right) = \left(\frac{q}{\mathfrak{p}}\right)^g.$$

Soumettons cette égalité à la substitution s^u, on a

$$(49) \qquad \left(\frac{s^u\pi}{\mathfrak{q}}\right) = \left(\frac{q}{s^u\mathfrak{p}}\right)^g.$$

Soient $p = ml + 1$, $p^* = m^*l + 1$, etc., les différents facteurs premiers de $n(\alpha)$; R, R*, ..., etc., des racines primitives mod p, p^*, ...; enfin, posons

$$\mathfrak{p} = (p, \zeta - \mathrm{R}^{-m}), \qquad \mathfrak{p}^* = (p, \zeta - \mathrm{R}^{*-m^*}), \ \ldots$$

et soit

$$\alpha = \mathfrak{p}^{\mathrm{F}(s)}\mathfrak{p}^{*\mathrm{F}^*(s)} \ldots$$

la décomposition du nombre α, les exposants $\mathrm{F}(s)$, $\mathrm{F}^*(s)$ ... étant des polynômes de degré $l - 2$ à coefficients entiers $\geqq 0$.

Λ, Λ^*, ... désignant les résolvantes de Lagrange relatives aux facteurs premiers p, p^*, ... et à leurs racines primitives R, R*, ..., en posant $\pi = \Lambda^l$, $\pi^* = \Lambda^{*l}$, ... on a, d'après le théorème 138, les décompositions

$$\pi = \mathfrak{p}^{r_0 + r_{-1}\cdot s + r_{-2}\cdot s^2 + \ldots + r_{-l+2}\cdot s^{l-2}},$$
$$\pi^* = \mathfrak{p}^{*r_0 + r_{-1}\cdot s + r_{-2}\cdot s^2 + \ldots + r_{-l+2}\cdot s^{l-2}},$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

où r_{-h} représente le plus petit entier positif congru à r^{-h} mod l (r racine primitive mod l).

Le quotient

$$\varepsilon = \frac{\alpha^{r_0 + r_{-1}\cdot s + \ldots + r_{-l+2}\cdot s^{l-2}}}{\pi^{\mathrm{F}(s)}\,\pi^{*\mathrm{F}^*(s)}\ldots}$$

est par suite, évidemment, une unité du corps $c(\zeta)$.

Nous allons démontrer que $\varepsilon = \pm 1$. Pour cela, formons $|\varepsilon|^2$:

$$|\varepsilon|^2 = \varepsilon^{1 + s^{\frac{l-1}{2}}} = \frac{\alpha^{\left(1 + s^{\frac{l-1}{2}}\right)(r_0 + r_{-1}\cdot s + \ldots + r_{-l+2}\cdot s^{l-2})}}{(|\pi|^2)^{\mathrm{F}(s)}(|\pi^*|^2)^{\mathrm{F}^*(s)}\ldots}.$$

A cause de l'égalité, valable pour $h = 0, 1, 2, \ldots, \frac{l-3}{2}$,

$$r_{-h} + r_{-h-\frac{l-1}{2}} = l,$$

le numérateur de la fraction du second membre est égal à

$$\alpha^{l(1+s+\ldots+s^{l-2})} = \big(n(\alpha)\big)^l.$$

Tenons compte de ce que (théorème 138) on a $|\pi|^2 = p^l$, $|\pi^*|^2 = p^{*l}$, ..., alors $|\varepsilon| = +1$. D'après le théorème 48, ε est donc à un facteur ± 1 près une puissance de ζ. Comme d'autre part on a, d'après le théorème 138,

$$\pi \equiv -1, \quad \pi^* \equiv -1, \quad \ldots \quad (\mathfrak{l}^2),$$

et que, par suite, $\pi, \pi^{*\prime}$, ... sont tous des nombres semi-primaires, il en est de même de ε; donc $\varepsilon = \pm 1$ et il en résulte

$$\alpha^{r_0 + r_{-1}s + \ldots + r_{-l+2}s^{l-2}} = \pm \pi^{F(s)} \pi^{*F^*(s)} \ldots .$$

Cette égalité donne, vu la formule (49), la relation de réciprocité

(50) $$\left(\frac{\alpha^{r_0 + r_{-1}s + \ldots + r_{-l+2}s^{l-2}}}{\mathfrak{q}}\right) = \left(\frac{q}{\mathfrak{p}^{F(s)}\mathfrak{p}^{*F^*(s)}\ldots}\right) = \left(\frac{q}{\alpha}\right)^q.$$

En tenant compte de ce que l'on a

$$\left(\frac{s\alpha}{\mathfrak{q}}\right) = \left(\frac{\alpha}{s^{-1}\mathfrak{q}}\right)^r, \quad \left(\frac{s^2\alpha}{\mathfrak{q}}\right) = \left(\frac{\alpha}{s^{-2}\mathfrak{q}}\right)^{r^2}, \quad \ldots,$$

puisque ces symboles représentent des puissances de ζ, il résulte de (50) l'égalité

$$\left(\frac{\alpha}{q^q}\right) = \left(\frac{q}{\alpha}\right)^q \quad \text{ou} \quad \left(\frac{\alpha}{q}\right) = \left(\frac{q}{\alpha}\right),$$

ce qui démontre le théorème 140 dans le cas particulier où α ne contient que des idéaux du premier degré et où q est un nombre premier.

Pour supprimer la première restriction, supposons maintenant que α soit un nombre semi-primaire quelconque, premier à q, de $c(\zeta)$, pouvant contenir des idéaux premiers de degré supérieur au premier. Formons alors le nombre

$$\beta = \alpha^{\Pi(1-s^e)},$$

le produit Π étant étendu à tous les diviseurs de $l-1$ différents de $l-1$, et posons

$$\beta = \frac{\mathfrak{j}}{\mathfrak{t}},$$

$\mathfrak{j}$ et $\mathfrak{t}$ étant des idéaux premiers entre eux; ces derniers ne peuvent contenir, on le

voit aisément, que des idéaux premiers du premier degré et, de plus, ne sont pas divisibles par $\mathfrak{l}$. Si h est le nombre des classes d'idéaux du corps $c(\zeta)$, on a, d'après le théorème 51, $\mathfrak{t}^h = (\varkappa)$, $\varkappa$ étant un entier de $c(\zeta)$; si nous posons $\gamma = \beta\varkappa^l$, γ est aussi un entier de $c(\zeta)$ n'ayant que des idéaux premiers du premier degré, et, de plus, γ est, de même que α, semi-primaire et premier à q. De ce qui précède résulte donc

$$(51)\qquad \left(\frac{\gamma}{q}\right) = \left(\frac{q}{\gamma}\right).$$

Dans un but de simplification, nous écrirons d'une manière générale, ρ et σ étant deux entiers de $c(\zeta)$ premiers à q,

$$\frac{\left(\frac{\rho}{q}\right)}{\left(\frac{\sigma}{q}\right)} = \left\{\frac{\frac{\rho}{\sigma}}{q}\right\} \quad \text{et} \quad \frac{\left(\frac{q}{\rho}\right)}{\left(\frac{q}{\sigma}\right)} = \left\{\frac{q}{\frac{\rho}{\sigma}}\right\},$$

ce qui est compatible avec les conventions déjà faites; alors, vu $\beta = \frac{\gamma}{\varkappa^l}$, on tire de (51) :

$$(52)\qquad \left(\frac{\beta}{q}\right) = \left(\frac{q}{\beta}\right).$$

En tenant compte des égalités

$$\left(\frac{s^u\alpha}{q}\right) = \left(\frac{\alpha}{q}\right)^{r^u} \quad \text{et} \quad \left(\frac{q}{s^u\alpha}\right) = \left(\frac{q}{\alpha}\right)^{r^u},$$

on déduit de (52) que

$$\left(\frac{\alpha}{q}\right)^{\prod\limits_{(u)}(1-r^{-u})} = \left(\frac{q}{\alpha}\right)^{\prod\limits_{(u)}(1-r^{-u})}.$$

Si nous remarquons que l'exposant commun aux deux membres n'est pas divisible par l, nous en tirons

$$\left(\frac{\alpha}{q}\right) = \left(\frac{q}{\alpha}\right).$$

Admettons enfin que a premier à l et à α soit quelconque, et que $a = qq^* \ldots$, $q, q^*, \ldots$; étant des nombres premiers, la multiplication des égalités

$$\left(\frac{q}{\alpha}\right) = \left(\frac{\alpha}{q}\right), \quad \left(\frac{q^*}{\alpha}\right) = \left(\frac{\alpha}{q^*}\right), \quad \ldots,$$

achève la démonstration du théorème 140.

CHAPITRE XXVI.

Détermination du nombre des classes d'idéaux.

§ 116. — Le symbole $\left[\frac{a}{\mathrm{L}}\right]$.

Pour appliquer au cas du corps circulaire $c\left(e^{\frac{2i\pi}{m}}\right)$, m étant quelconque, la méthode transcendante du paragraphe 26 pour la détermination du nombre des classes, définissons d'abord les *symboles* suivants :

Soit l^h une puissance d'exposant positif du nombre premier impair l, et r une racine primitive mod l^h, a étant alors un entier rationnel non divisible par l, et a' un exposant tel que

$$r^{a'} \equiv a, \quad (l^h),$$

nous poserons

$$\left[\frac{a}{l^h}\right] = e^{\frac{2i\pi a'}{l^{h-1}(l-1)}}.$$

Nous poserons en outre

$$\left[\frac{a}{l^h}\right] = 0$$

quand a sera divisible par l; a et b étant deux entiers rationnels quelconques, on a dès lors :

$$\left[\frac{ab}{l^h}\right] = \left[\frac{a}{l^h}\right]\left[\frac{b}{l^h}\right].$$

Nous poserons encore, a étant impair,

$$\left[\frac{a}{2^2}\right] = (-1)^{\frac{a-1}{2}},$$

et pour $h > 2$, a' étant un entier tel que

$$5^{a'} \equiv \pm a, \quad (2^h),$$

$$\left[\frac{a}{2^h}\right] = e^{\frac{2i\pi a'}{2^{h-2}}}.$$

Enfin, a étant pair, nous posons

$$\left[\frac{a}{2^2}\right] = 0, \quad \left[\frac{a}{2^h}\right] = 0, \quad (h > 2).$$

a et b étant deux nombres rationnels quelconques, on a donc

$$\left[\frac{ab}{2^h}\right]=\left[\frac{a}{2^h}\right]\left[\frac{b}{2^h}\right], \quad (h>1).$$

Ces conventions fixent complètement le sens du symbole $\left[\frac{a}{\mathrm{L}}\right]$, lorsque a est un entier quelconque et L soit une puissance de 2 supérieure à la seconde, soit une puissance de nombre premier impair, une racine primitive r pour le module L étant alors choisie une fois pour toutes.

$l_1^{h_1}$, $l_2^{h_2}$, ... étant des puissances déterminées de divers nombres premiers impairs et 2^{h^*} une puissance de 2 supérieure à 2^2, nous poserons pour abréger :

$$\left[\frac{a}{\underbrace{u_1, u_2, \ldots}}\right]=\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\ldots,$$

$$\left[\frac{a}{\underbrace{u; u_1, u_2, \ldots}}\right]=\left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\left[\frac{a}{l_2^{h_2}}\right]^{u_2}\ldots,$$

$$\left[\frac{a}{\underbrace{u, u^*; u_1, u_2, \ldots}}\right]=\left[\frac{a}{2^2}\right]^{u}\left[\frac{a}{2^{h^*}}\right]^{u^*}\left[\frac{a}{l_1^{h_1}}\right]^{u_1}\ldots,$$

a étant un nombre entier quelconque et les exposants $u, u^*; u_1, u_2, \ldots$ des entiers non négatifs. Enfin, nous conviendrons que $\left[\frac{a}{\mathrm{L}}\right]^0$ sera égal à 1, même si $\left[\frac{a}{\mathrm{L}}\right]=0$.

§ 117. — Expression du nombre des classes dans le corps circulaire des racines $m^{\text{ièmes}}$ de l'unité.

On a le théorème suivant, qui sera démontré au paragraphe 118.

Théorème 141. — Soit m un entier positif de la forme

$$m=l_1^{h_1}l_2^{h_2}\ldots, \quad \text{ou} \quad =2^2 l_1^{h_1}l_2^{h_2}\ldots, \quad \text{ou} \quad =2^{h^*} l_1^{h_1}l_2^{h_2}\ldots$$
$$(h^*>2,\ h_1>0,\ h_2>0\ \ldots),$$

où $l_1, l_2, \ldots$ sont des nombres premiers impairs distincts. Soient de plus $r_1, r_2, \ldots$, des racines primitives mod $l_1^{h_1}$, $l_2^{h_2}$, ..., avec les symboles qu'elles définissent. Le nombre de classes H du corps c des racines $m^{\text{ièmes}}$ de l'unité peut alors s'exprimer de deux façons :

La *première* expression de H est

$$\mathrm{H}=\frac{1}{w}\prod_{(u_1, u_2, \ldots)}\ \operatorname{Lim}_{s=1}\prod_{(p)}\frac{1}{1-\left[\frac{p}{\underbrace{u_1, u_2, \ldots}}\right]p},$$

ou par la même formule où l'on substitue à $u_1, u_2, \ldots, u; u_1, u_2, \ldots$, ou $u, u^*; u_1, u_2, \ldots$; (selon l'expression de m). Le produit extérieur doit être étendu aux nombres

$$(53)\qquad \begin{cases} u_1 = 0, 1, \ldots, l_1^{h_1-1}(l_1 - 1) - 1, \\ u_2 = 0, 1, \ldots, l_2^{h_2-1}(l_2 - 1) - 1, \\ \ldots\ldots\ldots\ldots\ldots \\ \text{et, s'il y a lieu, à} \\ u = 0, 1, \\ \text{et à} \\ u^* = 0, 1, \ldots, 2^{h-2} - 1, \end{cases}$$

à l'exception de la combinaison $u_1 = u_2 = \ldots = 0$; *ou* $u = u_1 = u_2 = \ldots = 0$; *ou* $u = u^* = u_1 = \ldots = 0$. Il comprend donc un nombre limité de facteurs. Chaque produit intérieur $\prod_{(p)}$ doit être étendu à tous les nombres premiers p, c'est donc un produit infini; $\varkappa$ est le nombre du corps c défini au théorème 56.

La *deuxième* expression de H est un produit de deux facteurs de forme fractionnaire :

$$H = \frac{\prod\limits_{(u_1, u_2, \ldots)} \sum\limits_{(n)} \left[\overbrace{u_1, u_2, \ldots}^{n}\right] n}{(2m)^{\frac{1}{2}\psi(m)-1}} \cdot \frac{\prod\limits_{(u_1, u_2, \ldots)} \sum\limits_{(n)} \left[\overbrace{u_1, u_2, \ldots}^{n}\right] \log A_n}{R}$$

(pour les autres expressions de m, on remplace $u_1, u_2, \ldots$ par $u; u_1, u_2, \ldots$; ou par $u, u^*; u_1, u_2, \ldots$ suivant le cas). Le produit Π au numérateur de la première fraction doit être étendu à toutes les valeurs données dans (53), pour lesquelles $u_1 + u_2 + \ldots$, dans le premier cas, et dans les deux autres cas $u + u_1 + u_2 + \ldots$, est un nombre impair; le produit Π au numérateur de la deuxième fraction est étendu à toutes les valeurs (53) pour lesquelles $u_1 + u_2 + \ldots$, dans le premier cas, $u + u_1 + u_2 + \ldots$, dans les deux autres, est un nombre pair, à l'exception de la seule combinaison $u_1 = u_2 = \ldots = 0$; ou $u = u_1 = u_2 \ldots = 0$; ou $u = u^* = u_1 = u_2 = \ldots = 0$. Chaque somme $\sum\limits_{(n)}$ de la première fraction est étendue à tous les entiers positifs $n = 1, \ldots, m - 1$; chaque somme $\sum\limits_{(n)}$ de la seconde fraction seulement à ceux de ces nombres qui sont $< \frac{m}{2}$. Enfin, $\log A_n$ représente la partie réelle du logarithme du nombre du corps circulaire

$$A_n = \sqrt{\left(1 - e^{\frac{2i\pi n}{m}}\right)\left(1 - e^{-\frac{2i\pi n}{m}}\right)}$$

et R est le régulateur du corps circulaire. [Kummer[22, 23].]

Kummer a appelé les deux fractions qui composent la seconde expression de H le *premier* et le *second facteur du nombre des classes*. Le double du premier facteur et le second sont toujours des nombres entiers. [Kronecker[9].]

Weber a démontré, en partant de la seconde expression de H, que le nombre de classes du corps circulaire des 2^hièmes racines de l'unité est toujours un nombre impair. [Weber[1, 4].]

Cette deuxième expression de H peut encore être transformée. Dans le cas où $m = l$ est un nombre premier impair, un petit calcul(1) conduit au théorème suivant :

THÉORÈME 142. — Si l est premier impair, le nombre de classes h du corps circulaire des racines $l^{\text{ièmes}}$ de l'unité est donné par

$$h = \frac{\prod\limits_{(n)} \sum\limits_{(n)} n\, e^{\frac{2i\pi n' n}{l-1}}}{(2l)^{\frac{l-3}{2}}} \cdot \frac{\Delta}{R}.$$

Le produit $\prod\limits_{(n)}$ est étendu aux nombres impairs $1, 3, \ldots\, l-2$, et chaque somme $\sum\limits_{(n)}$ aux nombres $n = 1, 2, \ldots\, l-1$; de plus, étant donnée une racine primitive r, mod l, n' désigne un nombre tel que $r^{n'} \equiv n$, mod l ; Δ désigne le déterminant

$$(-1)^{\frac{(l-1)(l-3)}{8}} \begin{vmatrix} \log \varepsilon_1, & \log \varepsilon_2, & \ldots, & \log \varepsilon_{\frac{l-3}{2}} \\ \log \varepsilon_2, & \log \varepsilon_3, & \ldots, & \log \varepsilon_{\frac{l-1}{2}} \\ \cdot & \cdot & \cdot & \cdot \\ \log \varepsilon_{\frac{l-3}{2}}, & \log \varepsilon_{\frac{l-1}{2}}, & \ldots, & \log \varepsilon_{l-4} \end{vmatrix},$$

où $\log \varepsilon_g$ représente la partie réelle du logarithme de l'unité

$$\varepsilon_g = \sqrt{\frac{1-\zeta^{r^g}}{1-\zeta^{r^{g-1}}} \cdot \frac{1-\zeta^{-r^g}}{1-\zeta^{-r^{g-1}}}},$$

ζ étant égal à $e^{\frac{2i\pi}{l}}$. [Kummer[7, 11], Dedekind[1].]

Les deux fractions de cette expression de h proviennent des deux fractions de la forme générale et sont par suite le premier et le second facteur du nombre de classes, dans le sens primitif ; dans le cas actuel, ces deux facteurs sont tous les deux entiers. Le second facteur représente le nombre de classes du sous-corps réel de degré $\frac{l-1}{2}$ contenu dans $c(\zeta)$. Kummer a encore établi d'autres théorèmes concernant la divisibilité par 2 de ces facteurs. [Kummer[25].] La tentative de Kronecker pour démontrer ces théorèmes par une voie purement arithmétique contient une erreur, et la généralisation donnée par Kronecker n'est pas exacte. [Kronecker[11].] En outre, Kummer a fait des recherches d'un autre ordre sur la signification et les propriétés de ces deux facteurs [Kummer[13].] (Voir chap. XXXVI.) Enfin, Kummer a énoncé le théorème que le nombre de classes de tout sous-corps de $c(\zeta)$ divise le nombre de classes h de $c(\zeta)$. La démonstration qu'il a essayée d'en donner n'est cependant pas inattaquable. [Kummer[7].]

(1) Voir la note I à la fin du Mémoire.

24

§ 118. — Démonstration des formules du nombre des classes de $k(e^{\frac{2i\pi}{m}})$.

Pour démontrer le théorème 141, prenons le cas le plus compliqué, où m est divisible par 8, et établissons le lemme suivant :

Lemme 22. — p étant un nombre premier quelconque et m un entier divisible par 8, on a, avec les notations du théorème 141, pour les valeurs réelles de $s > 1$, la formule

$$\prod_{(\mathfrak{P})}\{1 - n(\mathfrak{P})^{-s}\} = \prod_{(u, u^*;\, u_1, u_2, \dots)}\left\{1 - \left[\frac{p}{u, u^*;\, u_1, u_2, \dots}\right]p^{-s}\right\},$$

où le produit du premier membre est étendu à tous les idéaux premiers facteurs de p dans le corps $k(\zeta = e^{\frac{2i\pi}{m}})$, et où le produit du second membre est étendu à toutes les valeurs (53) [*y compris la combinaison* $u = u^* = u_1 = u_2 = \dots = 0$].

Démonstration. — Soit d'abord p un nombre premier ne divisant pas m ; soit l un des nombres premiers impairs $l_1, l_2, \dots,$ et l^h la puissance de l qui figure dans m ; soit r une racine primitive mod l^h et $p \equiv r^{p'}$, mod l^h. Si e désigne le plus grand commun diviseur des nombres p' et $l^{h-1}(l-1)$ et si l'on pose $l^{h-1}(l-1) = ef$, le symbole $\left[\frac{p}{l^h}\right]$ est évidemment exactement une $f^{\text{ième}}$ racine de l'unité et non une inférieure.

Si nous prenons d'abord $l = l_1$, et, par suite, $h = h_1$, $e = e_1$, $l_1^{h_1-1}(l_1-1) = e_1f_1$, on a la formule

$$\prod_{(u_1)}\left\{1 - \left[\frac{p}{u, u^*;\, u_1, u_2, \dots}\right]p^{-s}\right\} = \left\{1 - \left[\frac{p}{u, u^*;\, u_2, u_3, \dots}\right]^{f_1}p^{-sf_1}\right\}^{e_1},$$

où le produit est étendu à toutes les valeurs de u_1 indiquées dans (53)[1]. Si nous

---

[1] N. T. — C'est-à-dire : $u_1 = 0, 1, \dots, l_1^{h_1-1}(l_1-1) - 1$.

On a, en effet :

$$\left[\frac{p}{u, u^*;\, u_1, u_2, \dots}\right] = \left[\frac{p}{u, u^*;\, u_2, \dots}\right]\left[\frac{p}{l_1^{h_1}}\right]^{u_1} \quad \text{et} \quad \left[\frac{p}{l_1^{h_1}}\right] = \vartheta_1, \text{ avec } \vartheta_1^{f_1} = 1 ;$$

donc, en posant pour abréger :

$$q = \left[\frac{p}{u, u^*;\, u_2, \dots}\right],$$

on a :

$$\prod_{(u_1)} = \left(1 - \frac{q}{p^s}\right)\left(1 - \frac{q}{p^s}\vartheta_1\right)\left(1 - \frac{q}{p^s}\vartheta_1^2\right)\dots\left(1 - \frac{q}{p^s}\vartheta_1^{e_1f_1-1}\right)$$
$$= \left(1 - \frac{q}{p^s}\vartheta_1\right)\left(1 - \frac{q}{p^s}\vartheta_1^2\right)\dots\left(1 - \frac{q}{p^s}\vartheta_1^{e_1f_1}\right)$$
$$= \left[1 - \left(\frac{q}{p^s}\right)^{f_1}\right]^{e_1}.$$

prenons ensuite $l = l_2$ et $h = h_2$, $e = e_2$, $l_2^{h_2-1}(l_2 - 1) = e_2 f_2$, on a, f_{12} désignant le plus petit commun multiple de f_1 et f_2,

$$\prod_{(u_1, u_2)} \left\{ 1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots} \right] p^{-s} \right\} = \left\{ 1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots} \right]^{f_{12}} p^{-sf_{12}} \right\}^{\frac{e_1 e_2 f_1 f_2}{f_{12}}},$$

et ainsi de suite, — $f_{12\ldots}$ désignant le plus petit commun multiple des nombres $f_1, f_2, \ldots$

$$\prod_{(u_1, u_2, \ldots)} \left\{ 1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots} \right] p^{-s} \right\} = \left\{ 1 - \left[\frac{p}{u, u^*} \right]^{f_{12\ldots}} p^{-sf_{12\ldots}} \right\}^{\frac{e_1 e_2 \ldots f_1 f_2 \ldots}{f_{12\ldots}}}$$

où le produit est étendu à toutes les valeurs (53) de $u_1, u_2 \ldots$.

Soit de plus $p \equiv \pm 5^{p'}$, mod 2^h ; soit e^* le plus grand commun diviseur des nombres p' et 2^{h-2}, et soit $2^{h-2} = e^* f^*$: alors $\left[\frac{p}{2^h} \right]$ est évidemment exactement égal à une racine $f^{*\text{ième}}$ de l'unité et non à une inférieure. Par suite, si $f^*_{12\ldots} \ldots$ désigne le plus petit commun multiple de $f^*, f_1, f_2, \ldots$:

$$\prod_{(u^*, u_1, u_2, \ldots)} \left\{ 1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots} \right] p^{-s} \right\} = \left\{ 1 - \left[\frac{p}{2^2} \right]^{u f^*_{12\ldots}} p^{-sf^*_{12\ldots}} \right\}^{\frac{e^* e_1 e_2 \ldots f^* f_1 f_2 \ldots}{f^*_{12\ldots}}}.$$

Enfin, soit $\bar{e}$ le plus grand commun diviseur de $\frac{p-1}{2}$ et de 2, et posons $2 = \bar{e}\bar{f}$; il résulte alors de la dernière formule, si F désigne le plus petit commun multiple des nombres $\bar{f}, f^*, f_1, f_2, \ldots$ et si l'on pose pour abréger

$$E = \frac{\bar{e} e^* e_1 e_2 \ldots \bar{f} f^* f_1 f_2 \ldots}{F},$$

$$(54) \qquad \prod_{(u, u^*, u_1, u_2, \ldots)} \left\{ 1 - \left[\frac{p}{u, u^*; u_1, u_2, \ldots} \right] p^{-s} \right\} = \{ 1 - p^{-sF} \}^{E},$$

où le produit est étendu à toutes les combinaisons (53) de $u, u^*; u_1, u_2, \ldots$. On voit de suite que F est le plus petit exposant positif tel que $p^F \equiv 1$, mod m. Comme de plus $FE = \Phi(m)$, on déduit de (54), en ayant égard au théorème 125, la formule du lemme 22 [1]. En s'appuyant sur la deuxième partie du théorème 125, on reconnaît l'exactitude de cette formule même dans le cas où p divise m.

---

[1] N. T. — On a, en effet :

$$p^{\Phi(m)} = p^{EF} = n(p) = n(\mathfrak{P}_1) \ldots n(\mathfrak{P}_E). \qquad \text{(Théorème 125.)}$$

et

$$\prod_{(\mathfrak{P})} \left\{ 1 - \frac{1}{n(\mathfrak{P})^s} \right\} = \left[1 - \frac{1}{n(\mathfrak{P}_1)^s} \right] \left[1 - \frac{1}{n(\mathfrak{P}_2)^s} \right] \ldots \left[1 - \frac{1}{n(\mathfrak{P}_E)^s} \right]$$

$$= \left[1 - \frac{1}{p^{Fs}} \right] \left[1 - \frac{1}{p^{Fs}} \right] \ldots \left[1 - \frac{1}{p^{Fs}} \right]$$

$$= \left[1 - p^{-sF} \right]^{E}.$$

L'on voit alors immédiatement l'exactitude de la première expression de H donnée au théorème 141, en s'appuyant sur le théorème 56, la deuxième expression de $\zeta(s)$ donnée au paragraphe 27 et le lemme 22 qu'on vient de démontrer.

Pour obtenir la deuxième expression de H, nous transformons d'abord de la façon suivante le produit précédé du signe Lim de la première expression :

$$\prod_{(p)} \frac{1}{1-\left[\dfrac{p}{u,\, u^*;\, u_1,\, u_2,\, \ldots}\right] p^{-s}} = \sum_{(n=1,\,2,\,3,\,\ldots)} \left[\frac{n}{u,\, u^*;\, u_1,\, u_2,\, \ldots}\right] \frac{1}{n^s}.$$

La transformation de la somme du second membre s'opère ensuite de la façon la plus simple, si l'on pose

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^{\infty} e^{-nt} t^{s-1} dt$$

et que l'on procède comme au paragraphe 86 (1).

§ 119. Existence d'une infinité de nombres premiers qui ont pour un nombre donné un reste donné premier à ce dernier.

Chacune des deux expressions (théorème 141) du nombre de classes H du corps circulaire des racines conduit à une conséquence importante. La première sert en effet à démontrer le théorème suivant :

Théorème 143. — *m et n étant deux entiers premiers entre eux, il existe toujours une infinité de nombres premiers p vérifiant la congruence $p \equiv n$. mod m.* [Dirichlet[5,6], Dedekind[1].]

Démonstration. — Considérons encore seulement le cas le plus compliqué, où m est divisible par 8, et posons, comme au paragraphe 117, $m = 2^{h_0} l_1^{h_1} l_2^{h_2} \ldots$. Chacun des produits considérés

$$\prod_{(p)} \frac{1}{1-\left[\dfrac{p}{u,\, u^*;\, u_1,\, u_2,\, \ldots}\right] p^{-s}},$$

à l'exception de celui qui correspond à la combinaison $u = u^* = u_1 = u_2 = \ldots = 0$, a pour $s = 1$ une limite déterminée; de la première expression du nombre de classes H, donnée au paragraphe 117, résulte que ces limites sont toutes différentes

(1) N. T. — Nous donnons dans la note V, à la fin du Mémoire, le détail de ces calculs pour le cas simple où m est un nombre premier impair.

de o; nous pouvons donc prendre les logarithmes de ces produits, et on est alors conduit par des considérations simples, analogues à celles du paragraphe 80, à ce résultat, que pour tout système de valeurs u, u^* : u_1, u_2, ... (o partout exclus), la somme

$$(55)\qquad \sum_{(p)} \left[\frac{p}{u,\ u^*;\ u_1,\ u_2,\ \ldots}\right] \frac{1}{p^s},$$

où p parcourt toute la série des nombres premiers a une limite finie pour $s=1$.

Comme n est supposé premier à m, tous les symboles

$$\left[\frac{n}{2^2}\right],\quad \left[\frac{n}{2^h}\right],\quad \left[\frac{n}{l_1^{h_1}}\right],\quad \left[\frac{n}{l_2^{h_2}}\right],\quad \ldots$$

sont différents de o. Nous multiplions l'expression (55) par

$$\frac{1}{\left[\frac{n}{2^2}\right]^u \left[\frac{n}{2^h}\right]^{u^*} \left[\frac{n}{l_1^{h_1}}\right]^{u_1} \left[\frac{n}{l_2^{h_2}}\right]^{u_2} \cdots};$$

nous donnons à u, u^* ; u_1, u_2, ... toutes les valeurs (53), la combinaison o partout étant exclue, et nous ajoutons toutes les expressions ainsi formées à la série (26) (voir § 80). On obtient ainsi l'expression

$$(56)\qquad \left\{\begin{aligned} &\sum_{(p)} (1+\mathrm{P})(1+\mathrm{P}^*+\mathrm{P}^{*2}+\ldots+\mathrm{P}^{*(2^{h^*-2}-1)}).\\ &\qquad (1+\mathrm{P}_1+\mathrm{P}_1^2+\ldots+\mathrm{P}_1^{l_1^{h_1-1}(l_1-1)-1}).\\ &\qquad (1+\mathrm{P}_2+\mathrm{P}_2^2+\ldots+\mathrm{P}_2^{l_2^{h_2-1}(l_2-1)-1})\ldots\frac{1}{p^s}, \end{aligned}\right.$$

où l'on a posé pour abréger

$$\mathrm{P}=\frac{\left[\frac{p}{2^2}\right]}{\left[\frac{n}{2^2}\right]},\quad \mathrm{P}^*=\frac{\left[\frac{p}{2^h}\right]}{\left[\frac{n}{2^h}\right]},\quad \mathrm{P}_1=\frac{\left[\frac{p}{l_1^{h_1}}\right]}{\left[\frac{n}{l_1^{h_1}}\right]},\quad \ldots.$$

Si nous faisons abstraction dans cette série des termes, en nombre limité, correspondant aux facteurs premiers de m : 2, l_1, l_2, ..., le reste est égal à $\Phi_m \sum \frac{1}{p^s}$, où p représente les nombres premiers, tels que tous les symboles P, P^*, P_1, P_2, ... soient égaux à 1, c'est-à-dire les nombres premiers vérifiant la congruence du théorème 143.

Comme la série (26) est infinie pour $s=1$, tandis que les séries (55) restent toutes finies pour $s=1$, il en résulte que la série (56) est aussi infinie pour $s=1$, c'est-à-dire qu'il y a une infinité de nombres premiers vérifiant la congruence.

§ 120. — Représentation de toutes les unités du corps circulaire au moyen d'unités circulaires.

La deuxième expression du paragraphe 117 peut servir à démontrer le théorème suivant :

Théorème 144. — *Toute unité d'un corps abélien est une puissance fractionnaire d'un produit d'unités circulaires.*

Démonstration. — Prenons d'abord le cas où $m = l$ est premier impair. D'après la formule du théorème 142, le second facteur du nombre de classes contient au numérateur un certain déterminant Δ. Ce dernier est donc nécessairement $\neq 0$, d'où il suit, vu les considérations des paragraphes 20 et 21, que les $\frac{l-3}{2}$ unités $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{\frac{l-3}{2}}$ du théorème 142 forment un système d'unités indépendantes du corps circulaire $c(e^{\frac{2i\pi}{l}})$. Ceci montre l'exactitude du théorème 144 pour le cas particulier du corps circulaire $c(e^{\frac{2i\pi}{l}})$ et, par suite, pour tous les sous-corps qu'il contient. [Kummer[11].]

On peut transformer le second facteur du nombre de classes, comme au théorème 142, même dans le cas où m est composé ; l'expression obtenue conduit alors, avec le théorème 131, à la démonstration générale du théorème 144.

Les tables de nombres premiers complexes calculées par Reuschle constituent une mine abondante de valeurs numériques, de la plus grande utilité pour des recherches plus approfondies sur les corps circulaires. [Reuschle[1], Kummer[24], Kronecker[12].]

CHAPITRE XXVII.

Applications aux corps quadratiques.

§ 121. — Expression des unités d'un corps quadratique réel au moyen d'unités circulaires.

En utilisant quelques-unes des propriétés du corps circulaire des racines $m^{\text{ièmes}}$ de l'unité relatives à un de ses sous-corps quadratiques, nous arrivons à de nouveaux résultats relatifs aux corps quadratiques. La fécondité de cette méthode s'accroît encore, si on la combine avec les propriétés du corps quadratique déjà démontrées directement, dans la troisième partie.

D'après le théorème général 144, toute unité d'un corps quadratique réel $c(\sqrt{m})$ est puissance fractionnaire d'un produit d'unités circulaires; on obtient simplement une unité particulière du corps $c(\sqrt{m})$ au moyen de l'expression

$$\frac{\prod\limits_{(b)} \left(e^{\frac{bi\pi}{d}} - e^{-\frac{bi\pi}{d}}\right)}{\prod\limits_{(a)} \left(e^{\frac{ai\pi}{d}} - e^{-\frac{ai\pi}{d}}\right)},$$

où d est le discriminant du corps $c(\sqrt{m})$ et où les produits $\prod\limits_{(a)}$, $\prod\limits_{(b)}$ sont étendus à tous les nombres a ou b de la suite $1, 2, \ldots, d$, qui vérifient les conditions

$$\left(\frac{d}{a}\right) = +1, \qquad \left(\frac{d}{b}\right) = -1.$$

[Dirichlet[7].] Voir § 86.

§ 122. — Loi de réciprocité des résidus quadratiques.

Soit l un nombre premier impair, r une racine primitive, mod l; $\zeta = e^{\frac{2i\pi}{l}}$, $s = (\zeta : \zeta^r)$. Au sous-groupe des $\frac{l-1}{2}$ substitutions $1, s^2, s^4, \ldots, s^{l-3}$, de $c(\zeta)$, correspond un certain sous-corps quadratique c^* de $c(\zeta)$. Le discriminant du corps $c(\zeta)$ étant (théorème 118) $(-1)^{\frac{l-1}{2}} l^{l-2}$, le discriminant du corps c^* ne contient pas (théorème 39) d'autre facteur premier que l et a par suite, d'après le théorème 95, la valeur $d = (-1)^{\frac{l-1}{2}} l$.

Soit p le nombre premier 2 ou un nombre premier impair quelconque autre que l. En décomposant p d'une part dans le corps $c(\zeta)$ des racines $l^{\text{ièmes}}$ de l'unité, d'autre part directement d'après le théorème 97 dans le sous-corps quadratique c^*, et en comparant les résultats, on arrive à une nouvelle démonstration de la loi de réciprocité des résidus quadratiques. [Kronecker[15].] Nous procéderons comme suit :

f étant le plus petit exposant positif, pour lequel $p^f \equiv 1$, mod l, en posant $e = \frac{l-1}{f}$, p se décompose dans $c(\zeta)$ (théorème 119) en e idéaux premiers $\mathfrak{P}$, $s\mathfrak{P}, \ldots, s^{e-1}\mathfrak{P}$, et le corps de décomposition commun c_d de ces idéaux premiers est de degré e (théorème 129). Le nombre premier p est ensuite évidemment décomposable ou non dans le corps quadratique c^*, selon que c^* est contenu ou non dans c_d. En remarquant que le corps $c(\zeta)$ ne contient pas d'autre sous-corps quadratique que c^* et que de plus, pour qu'un corps abélien possède précisément un sous-corps quadratique, il faut et il suffit que son degré soit pair, on voit que pour

que c^* soit contenu dans c_d il faut et il suffit que e soit pair. D'autre part, d'après le théorème 97, p est ou non décomposable dans c^*, selon que l'on a

$$\left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right) = +1, \qquad \text{ou} \qquad = -1.$$

Or, si e est pair, on a

$$p^{\frac{l-1}{2}} = p^{f.\frac{e}{2}} \equiv 1, \quad \text{mod } l,$$

c'est-à-dire $\left(\frac{p}{l}\right) = +1$; sinon

$$p^{\frac{l-1}{2}} = p^{\frac{f}{2}.e} \equiv (-1)^e = -1, \quad \text{mod } l,$$

c'est-à-dire $\left(\frac{p}{l}\right) = -1$. On a donc toujours

(57) $$\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{p}\right).$$

Nous supposons d'abord p impair; de (57) résulte

(58) $$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right),$$

et, en échangeant p et l,

$$\left(\frac{(-1)^{\frac{l-1}{2}}}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{l}\right).$$

Cette dernière égalité donne en prenant $l = 3$:

(59) $$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

La réunion des égalités (58 et (59) donne

(60) $$\left(\frac{l}{p}\right)\left(\frac{p}{l}\right) = (-1)^{\frac{l-1}{2}.\frac{p-1}{2}}.$$

Si nous posons dans (57) $p = 2$, on a

(61) $$\left(\frac{2}{l}\right) = \left(\frac{(-1)^{\frac{l-1}{2}} l}{2}\right) = (-1)^{\frac{l^2-1}{8}}.$$

Les formules (60), (59) et (61) expriment la loi de réciprocité des résidus quadratiques, ainsi que les lois complémentaires.

§ 123. — Les corps quadratiques imaginaires de discriminant premier.

Théorème 145. — l étant un nombre premier $\equiv 3 \bmod 4$ et p un nombre premier de la forme $ml+1$, on a pour tout idéal premier $\mathfrak{p}$ facteur de p dans le corps quadratique imaginaire $c(\sqrt{-l})$ l'équivalence

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} \sim 1,$$

où Σa désigne la somme des plus petits résidus quadratiques positifs mod l, et Σb la somme des plus petits non-résidus.

En posant de plus $p = \mathfrak{p}\mathfrak{p}'$ et

$$\mathfrak{p}^{\frac{\Sigma b - \Sigma a}{l}} = (\pi),$$

où (π) est un entier du corps imaginaire $c(\sqrt{-l})$, on a la congruence

$$\pi \equiv \pm \frac{1}{\prod_{(a)} (am)!}, \quad (\mathfrak{p}'),$$

où le produit du dénominateur est étendu à tous les plus petits résidus quadratiques positifs a, mod l. [Jacobi[1, 2, 3, 4], Cauchy[1], Eisenstein[4].]

Démonstration. — D'après le théorème 136, on peut, $\mathfrak{P}$ étant un idéal premier du premier degré de $c(\zeta)$, poser, avec les notations y indiquées,

$$(62) \qquad \mathfrak{P}^{q_0 + q_{-1}s + \dots + q_{-l+2}s^{l-2}} = (\mathrm{A}).$$

A étant un entier de $c(\zeta)$. Si alors $p = ml + 1$ est le nombre premier divisible par $\mathfrak{P}$ et $p = \mathfrak{p}\mathfrak{p}'$, la décomposition de ce nombre premier dans le sous corps quadratique $c(\sqrt{-l})$ de $c(\zeta)$, ces deux idéaux premiers $\mathfrak{p}$, $\mathfrak{p}'$ de $c(\sqrt{-l})$ sont

$$\mathfrak{p} = \mathfrak{P}^{1+s^2+s^4+\dots+s^{l-3}},$$
$$\mathfrak{p}' = s\mathfrak{p} = \mathfrak{P}^{s(1+s^2+\dots+s^{l-3})}.$$

En élevant l'égalité (62) à la puissance symbolique $(1+s^2+\dots+s^{l-3})$, on obtient

$$\mathfrak{p}^{q_0+q_{-2}+\dots+q_{-l+3}}\mathfrak{p}'^{q_{-1}+q_{-3}+\dots+q_{-l+2}} = (\alpha),$$

où α est un nombre de $c(\sqrt{-l})$. A cause de

$$q_{-1} + q_{-3} + \dots + q_{-l+2} - q_0 - q_{-2} - \dots - q_{-l+3} = (r+1)\frac{\Sigma b - \Sigma a}{l},$$

on a, vu l'équivalence $\mathfrak{p}\mathfrak{p}' \sim 1$,

$$(63) \qquad \mathfrak{p}^{(r+1)\frac{\Sigma b - \Sigma a}{l}} \sim 1.$$

D'autre part, on peut poser (théorème 135)

$$\mathfrak{P}^{r_0 + r_1 s + \dots + r_{l-2} s^{l-2}} = (\mathsf{B}),$$

B étant un nombre de $c(\zeta)$. En élevant cette égalité à la $(1 + s^2 + \dots s^{l-3})^{\text{ième}}$ puissance symbolique, on en déduit

$$(64) \qquad \mathfrak{p}^{\Sigma b - \Sigma a} = \mathfrak{p}^{l\frac{\Sigma b - \Sigma a}{l}} \sim 1.$$

Comme $r+1$ n'est pas divisible par l, si nous mettons de côté le cas de $l = 3$, suffisamment clair par lui-même, il résulte des deux équivalences (63) et (64) celle du théorème 145.

La deuxième partie du théorème est une conséquence des propriétés (43) et (44) de la résolvante de Lagrange $\mathsf{\Lambda}$ démontrées au paragraphe 112.

On a une démonstration tout à fait différente de la première partie du théorème 145 en s'appuyant sur une remarque faite vers la fin du paragraphe 86, au sujet de l'expression du nombre de classes du corps $c(\sqrt{-l})$ dans le cas de $l \equiv 3$, mod 4.

On arrive même, par une modification remarquable de la méthode de Jacobi, à étendre l'énoncé du théorème 145 au cas où le nombre premier p n'est pas de la forme $ml + 1$. [Eisenstein[1], Stickelberger[1].]

§ 124. — Détermination du signe de la somme de Gauss.

Soit p un nombre premier impair, on peut obtenir, selon les définitions du paragraphe 111, étendues dans le paragraphe 112, la base normale de Lagrange et la résolvante de Lagrange, dans le cas de $l = 2$, pour le corps quadratique $c\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right)$.

Soit $\mathsf{Z} = e^{\frac{2i\pi}{p}}$. La base de Lagrange se compose pour ce corps des deux nombres

$$\lambda_0 = \sum_{(a)} \mathsf{Z}^a, \qquad \lambda_1 = \sum_{(b)} \mathsf{Z}^b,$$

et la résolvante de Lagrange est

$$\mathsf{\Lambda} = \lambda_0 - \lambda_1 = \sum_{(a)} \mathsf{Z}^a - \sum_{(b)} \mathsf{Z}^b,$$

a et b étant les résidus et non-résidus quadratiques de p compris dans $1, 2, \dots, p-1$.

Le problème indiqué à la fin du paragraphe 112, de la détermination complète de $\mathsf{\Lambda}$, une fois $\mathsf{\Lambda}^l$ trouvé, revient ici, dans le cas du corps quadratique, à la détermination d'un signe $\pm$, et la solution est la suivante :

Théorème 146. — La résolvante de Lagrange $\mathsf{\Lambda}$ du corps quadratique de discriminant premier $(-1)^{\frac{p-1}{2}} p$ est un nombre positif réel ou purement imaginaire positif. [Gauss[2], Kronecker[1].]

Démonstration. — Le carré de la racine de Lagrange en question $\mathsf{\Lambda}$ est toujours égal à $(-1)^{\frac{p-1}{2}}p$, parce que $\mathsf{\Lambda}$ est un nombre du corps quadratique et que, d'après le théorème 138,

$$\mathsf{\Lambda} = \pm\sqrt{p}.$$

On a donc

(65) $$\mathsf{\Lambda} = \pm\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Les idéaux $\mathfrak{p}$, $\mathfrak{P}$ du paragraphe 112 sont remplacés dans le cas actuel de $l = 2$ par (p) et $(1 - \mathsf{Z})$; la congruence (43) donne alors

$$\mathsf{\Lambda} \equiv \frac{(-1)^{\frac{p-1}{2}}}{\left(\frac{p-1}{2}\right)!}(1-\mathsf{Z})^{\frac{p-1}{2}}, \quad \text{mod } (1-\mathsf{Z})^{\frac{p+1}{2}}.$$

c'est-à-dire

(66) $$\mathsf{\Lambda} \equiv \left(\frac{p-1}{2}\right)!\,(1-\mathsf{Z})^{\frac{p-1}{2}}, \quad \text{mod } (1-\mathsf{Z})^{\frac{p+1}{2}}.$$

Considérons d'autre part l'expression

$$\Delta = (\mathsf{Z}^{-1} - \mathsf{Z})(\mathsf{Z}^{-2} - \mathsf{Z}^{2})\ldots(\mathsf{Z}^{-\frac{p-1}{2}} - \mathsf{Z}^{\frac{p-1}{2}}).$$

Comme cette dernière change seulement de signe lorsqu'on remplace Z par Z^{R}, R étant une racine primitive, mod p, et que l'idéal (Δ) coïncide avec l'idéal $(1 - \mathsf{Z})^{\frac{p-1}{2}}$, on a nécessairement

$$\Delta = \pm\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Pour déterminer le signe, remarquons que l'on a

$$\mathsf{Z}^{-h} - \mathsf{Z}^{h} = -2i\sin\frac{2h\pi}{p}, \qquad \left(h = 1, 2, \ldots, \frac{p-1}{2}\right)$$

et qu'on obtient par suite pour Δ une valeur de la forme $(-i)^{\frac{p-1}{2}}P$, où P est positif. Donc, en entendant par $\sqrt{(-1)^{\frac{p-1}{2}}p}$ celle des racines carrées qui est réelle positive ou positivement imaginaire, on a

(67) $$\Delta = (-1)^{\frac{p^2-1}{8}}\sqrt{(-1)^{\frac{p-1}{2}}p}.$$

Enfin, la relation

$$\Delta = Z^{-1-2-\cdots-\frac{p-1}{2}}(1-Z^2)(1-Z^4)\ldots(1-Z^{p-1}),$$

montre que l'on a

$$\Delta \equiv 2.4.6\ldots(p-1)(1-Z)^{\frac{p-1}{2}} \equiv 2^{\frac{p-1}{2}}\frac{p-1}{2}!(1-Z)^{\frac{p-1}{2}}, \quad \text{mod } (1-Z)^{\frac{p+1}{2}}$$

et par suite, vu (66),

$$\Delta \equiv 2^{\frac{p-1}{2}}\Lambda, \quad \text{mod } (1-Z)^{\frac{1+p}{2}}.$$

Comme l'on a

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}}, \quad (p),$$

on obtient, à cause de (67),

$$\Lambda \equiv \sqrt{(-1)^{\frac{p-1}{2}}p}, \quad \text{mod } (1-Z)^{\frac{p+1}{2}},$$

et par suite, à cause de (65),

$$\Lambda = \sqrt{(-1)^{\frac{p-1}{2}}p},$$

ce qui démontre le théorème 146.

On n'a pas encore publié beaucoup de travaux sur des corps abéliens de degré supérieur au second; mentionnons le travail d'Eisenstein sur les formes cubiques, provenant de la division du cercle, qui est une introduction à la théorie des corps abéliens cubiques [Eisenstein[10]], le travail de Bachmann[1] sur les nombres complexes composés de deux racines carrées, et enfin les recherches de Weber sur les corps abéliens cubiques et biquadratiques. [Weber[2, 4].]

CINQUIÈME PARTIE.

LES CORPS KUMMERIENS.

CHAPITRE XXVIII.

Décomposition des nombres d'un corps circulaire dans un corps kummerien.

§ 125. — DÉFINITION D'UN CORPS KUMMERIEN.

Soit l un nombre premier impair et $c(\zeta)$ le corps circulaire défini par $\zeta = e^{\frac{2i\pi}{l}}$. μ étant alors un entier de $c(\zeta)$, qui ne soit pas en même temps la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$, l'équation du $l^{\text{ième}}$ degré

$$x^l - \mu = 0$$

est irréductible dans le domaine de rationalité $c(\zeta)$. $\mathsf{M} = \sqrt[l]{\mu}$ étant une racine déterminée choisie arbitrairement de cette équation, les autres sont $\zeta\mathsf{M}$, $\zeta^2\mathsf{M}$, ..., $\zeta^{l-1}\mathsf{M}$. J'appellerai *corps kummerien* le corps déterminé par M et ζ. Un tel corps kummerien $c(\mathsf{M}, \zeta)$ est de degré $l(l-1)$; il contient $c(\zeta)$ comme sous-corps, et c'est, par rapport à ce dernier, un corps abélien relatif de degré l.

Le changement de M en $\zeta\mathsf{M}$ dans un nombre ou un idéal du corps kummerien donne le nombre ou l'idéal conjugués relatifs. Nous représenterons ce changement par la substitution S.

On démontre facilement les propositions :

THÉORÈME 147. — Pour que le corps kummerien engendré par $M = \sqrt[l]{\mu}$ et ζ soit un corps de Galois dans le domaine des nombres rationnels, il faut et il suffit que l'une des puissances symboliques μ^{s-1}, μ^{s-2}, ..., μ^{s-l+1} soit la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$. ($s = (\zeta : \zeta^r)$, r racine primitive, mod l.)

La condition nécessaire et suffisante pour qu'il soit abélien est que : μ^{s-r} soit la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$.

Lorsque le corps kummerien (M, ζ) est un corps de Galois, ou un corps abélien, il résulte, comme le montrent les considérations du paragraphe 38, de la composition du corps $c(\zeta)$ et d'un certain corps de degré l.

§ 126. — Discriminant relatif d'un corps kummerien.

Notre premier problème est celui de la détermination du discriminant relatif de $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$. Nous démontrerons d'abord la proposition suivante :

Lemme 23. — Si un idéal premier $\mathfrak{p}$ du corps circulaire $c(\zeta)$ est la $l^{\text{ième}}$ puissance d'un idéal premier $\mathfrak{P}$ du corps kummerien $c(\mathsf{M}, \zeta)$ et que A soit un entier de $c(\mathsf{M}, \zeta)$ divisible par $\mathfrak{P}$, mais non par $\mathfrak{P}^2$, le discriminant relatif du nombre A et celui du corps kummerien $c(\mathsf{M}, \zeta)$ par rapport au corps $c(\zeta)$ contiennent le facteur idéal $\mathfrak{p}$ à la même puissance.

Démonstration. — Tout entier du corps $c(\mathsf{M}, \zeta)$ peut être mis sous la forme

$$(68) \qquad \Omega = \frac{\alpha + \alpha_1\mathsf{A} + \alpha_2\mathsf{A}^2 + \ldots + \alpha_{l-1}\mathsf{A}^{l-1}}{\beta},$$

où $\alpha, \alpha_1, \ldots, \alpha_{l-1}, \beta$ sont des entiers de $c(\zeta)$. Si β est divisible par $\mathfrak{p}$, il en résulte que le numérateur de la fraction doit aussi être $\equiv 0$, mod $\mathfrak{p}$.

A cause de $\mathsf{A} \equiv 0$, mod $\mathfrak{P}$, on en conclut $\alpha \equiv 0$, mod $\mathfrak{P}$ et, comme α est dans $c(\zeta)$, également $\alpha \equiv 0$, mod $\mathfrak{p}$. Cette dernière congruence donne

$$\alpha_1\mathsf{A} + \alpha_2\mathsf{A}^2 + \ldots + \alpha_{l-1}\mathsf{A}^{l-1} \equiv 0, \quad (\text{mod } \mathfrak{p}),$$

et comme $\mathsf{A} \not\equiv 0$, $\mathsf{A}^2 \equiv 0$, $\mathsf{A}^3 \equiv 0, \ldots, \mathsf{A}^{l-1} \equiv 0$, mod $\mathfrak{p}$, on a $\alpha_1 \equiv 0$, mod P, et par suite aussi, mod $\mathfrak{p}$; on a donc aussi

$$\alpha_2\mathsf{A}^2 + \ldots + \alpha_{l-1}\mathsf{A}^{l-1} \equiv 0, \quad (\mathfrak{p}).$$

Comme $\mathsf{A}^2 \not\equiv 0$, $\mathsf{A}^3 \equiv 0, \ldots, \mathsf{A}^{l-1} \equiv 0$, mod $\mathfrak{P}^3$, on a $\alpha_2 \equiv 0$, mod $\mathfrak{P}$, et par suite aussi, mod $\mathfrak{p}$.

En continuant ainsi, nous voyons que tous les coefficients $\alpha, \alpha_1, \ldots, \alpha_{l-1}$ doivent être divisibles par $\mathfrak{p}$. Si maintenant β' est un entier de $c(\zeta)$, divisible par $\frac{\beta}{\mathfrak{p}}$, mais non par β, les nombres $\alpha\beta', \alpha_1\beta', \ldots, \alpha_{l-1}\beta'$ sont tous divisibles par β. En posant

$$\alpha' = \frac{\alpha\beta'}{\beta}, \qquad \alpha_1' = \frac{\alpha_1\beta'}{\beta}, \qquad \ldots, \qquad \alpha_{l-1}' = \frac{\alpha_{l-1}\beta'}{\beta},$$

nous obtenons

$$(69) \qquad \Omega = \frac{\alpha' + \alpha_1'\mathsf{A} + \alpha_2'\mathsf{A}^2 + \ldots + \alpha_{l-1}'\mathsf{A}^{l-1}}{\beta'},$$

où le nombre β' du dénominateur contient maintenant un facteur idéal $\mathfrak{p}$ de moins que β. En appliquant à (69) la même méthode qu'à (68) et ainsi de suite, nous arri-

vons finalement au résultat que tout entier Ω du corps $c(\mathsf{M}, \zeta)$ peut être mis sous la forme

$$(70) \qquad \Omega = \frac{\alpha + \alpha_1 \mathsf{A} + \ldots + \alpha_{l-1}\mathsf{A}^{l-1}}{\beta},$$

où $\overline{\alpha}, \overline{\alpha}_1, \ldots, \overline{\alpha}_{l-1}, \beta$ sont des entiers de $c(\zeta)$, $\overline{\beta}$ étant en outre premier à $\mathfrak{p}$. Supposons exprimés sous la forme (70) les $l(l-1)$ nombres d'une base du corps kummerien $c(\mathsf{M}, \zeta)$, et formons avec ces nombres et leurs conjugués relatifs la matrice à l lignes : il est alors visible que le discriminant relatif du corps kummerien $c(\mathsf{M}, \zeta)$ multiplié par certains entiers $\overline{\beta}$ premiers à $\mathfrak{p}$ de $c(\zeta)$ doit être divisible par le discriminant relatif du nombre A, ce qui démontre le lemme 23.

Théorème 148. — Soit $\lambda = 1 - \zeta$ et $\mathfrak{l} = (\lambda)$. Si un idéal premier $\mathfrak{p}$ autre que $\mathfrak{l}$ de $c(\zeta)$ entre exactement à la puissance e dans le nombre μ, le discriminant relatif du corps kummerien déterminé par $\mathsf{M} = \sqrt[l]{\mu}$ et ζ par rapport à $c(\zeta)$ contient en facteur exactement la puissance $\mathfrak{p}^{l-1}$ de $\mathfrak{p}$, si e et l sont premiers entre eux. Si, au contraire, e est un multiple de l, le discriminant relatif est premier à $\mathfrak{p}$.

Quant à l'idéal premier $\mathfrak{l}$, nous pouvons d'abord exclure le cas où μ est divisible par $\mathfrak{l}$ et contient cet idéal à une puissance dont l'exposant est un multiple de l; car alors le nombre μ pourrait être remplacé par un nombre μ^* premier à $\mathfrak{l}$, le corps $c\left(\sqrt[l]{\mu^*}, \zeta\right)$ restant le même que le corps $c\left(\sqrt[l]{\mu}, \zeta\right)$. En dehors de ce cas, μ peut contenir une puissance de $\mathfrak{l}$ dont l'exposant est premier à l, ou bien μ peut ne pas être divisible par $\mathfrak{l}$. Dans le premier cas, le discriminant relatif de $c\left(\sqrt[l]{\mu}, \zeta\right)$, par rapport à $c(\zeta)$, est exactement divisible par $\mathfrak{l}^{l^2-1}$. Dans le second cas, soit m le plus grand exposant $\leqslant l$ pour lequel il existe dans $c(\zeta)$ un nombre α, tel que $\mu \equiv \alpha^l \bmod \mathfrak{l}^m$. Le discriminant relatif est alors premier à $\mathfrak{l}$, dans le cas de $m = l$, et si $m < l$ il est divisible par la puissance $\mathfrak{l}^{(l-1)(l-m+1)}$ de $\mathfrak{l}$.

Démonstration. Première partie. — Soit π un nombre entier de $c(\zeta)$ divisible par $\mathfrak{p}$, mais non par $\mathfrak{p}^2$, et soit ν un nombre entier de $c(\zeta)$ divisible par $\dfrac{\pi}{\mathfrak{p}}$, mais premier à $\mathfrak{p}$.

Si l'exposant de la puissance de $\mathfrak{p}$ contenue dans μ n'est pas un multiple de l, on peut déterminer deux entiers a et b, tels que $1 = ae + bl$; alors $\mu^* = \dfrac{\mu^a \nu^{bl}}{\pi^{bl}}$ est un entier de $c(\zeta)$ divisible par $\mathfrak{p}$, mais non par $\mathfrak{p}^2$; et si l'on pose $\mathsf{M}^* = \sqrt[l]{\mu^*}$, on a $c(\mathsf{M}^*, \zeta) = c(\mathsf{M}, \zeta)$; et si l'on désigne par $\mathfrak{P}$ le plus grand commun diviseur idéal de $\mathfrak{p}$ et M^* dans $c(\mathsf{M}, \zeta)$, on a [1]

$$\mathfrak{P} = S\mathfrak{P}, \quad \mathfrak{p} = \mathfrak{P}^l.$$

---

[1] N. T. — Car $S\mathfrak{p} = \mathfrak{p}$, $S\mathsf{M}^* = \zeta\mathsf{M}^*$, et le plus grand commun diviseur de $\mathfrak{p}$ et de $\zeta\mathsf{M}^*$ est le même que celui de $\mathfrak{p}$ et de M^*, car ζ est une unité.

L'idéal $\mathfrak{P}$ est donc un idéal premier invariant du corps kummerien $c(\mathsf{M}, \zeta)$ par rapport au sous-corps $c(\zeta)$; d'après le théorème 93, il entre donc comme facteur dans le discriminant relatif de $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$. Comme de plus M^* est divisible par $\mathfrak{P}$, mais non par $\mathfrak{P}^2$, et que le discriminant relatif de M^*, par rapport à $c(\zeta)$, est égal à $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$, l'idéal $\mathfrak{p}$ est donc, d'après le lemme 23, contenu dans le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ exactement à la $l-1^{\text{ième}}$ puissance.

Si, au contraire, l'exposant e est un multiple de l, $\mu^* = \frac{\mu\nu^e}{\pi^e}$ est un entier de $c(\zeta)$ non divisible par $\mathfrak{p}$; comme le discriminant relatif du nombre $\mathsf{M}^* = \sqrt[l]{\mu^*}$ par rapport à $c(\zeta)$ est égal à $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$, il est premier à $\mathfrak{p}$. Il en est de même du discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$.

Deuxième partie. — Dans le cas où μ contient $\mathfrak{l}$ avec un exposant e, non multiple de l, procédons comme dans la première partie et prenons à la place de μ un nombre μ^*, divisible par $\mathfrak{l}$ et non par $\mathfrak{l}^2$. Comme le discriminant relatif du nombre $\mathsf{M}^* = \sqrt[l]{\mu^*}$ a la valeur $(-1)^{\frac{l-1}{2}} l^l \mu^{*l-1}$, le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$ est exactement divisible par $\mathfrak{l}^{l^2-1}$, d'après la nature du nombre μ^* et la lemme 23.

Nous avons en second lieu à examiner le cas où μ n'est pas divisible par $\mathfrak{l}$. Soit d'abord $m = l$; il y a donc dans $c(\zeta)$ un entier α, tel que $\mu \equiv \alpha^l$, mod $\mathfrak{l}^l$. $\frac{\mu - \alpha^l}{\lambda^l}$ est donc un entier de $c(\zeta)$, et, par suite, l'équation de degré l en x

$$\frac{(\lambda x - \alpha)^l + \mu}{\lambda^l} = 0$$

a tous ses coefficients entiers. Comme en posant $\mathsf{M} = \sqrt[l]{\mu}$, $x = \frac{\alpha - \mathsf{M}}{\lambda}$ est une racine de cette équation, $\Omega = \frac{\alpha - \mathsf{M}}{\lambda}$ est un entier du corps $c(\zeta)$. Le discriminant relatif de ce nombre Ω est égal à $\varepsilon\mu^{l-1}$, ε étant une unité, et, par suite, le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$ est aussi premier à $\mathfrak{l}$.

Soit ensuite $m < l$, de sorte que μ ne soit pas congru à une puissance $l^{\text{ième}}$, mod $\mathfrak{l}^l$; posons $\mu \equiv \alpha^l + a\lambda^m$, mod $\mathfrak{l}^{m+1}$, α étant un entier de $c(\zeta)$, m l'exposant défini dans l'énoncé et a un entier rationnel non divisible par l. Considérons alors l'idéal

$$\mathfrak{A} = (\lambda, \alpha - \mathsf{M}).$$

Le nombre $\frac{\alpha - \mathsf{M}}{\lambda}$ n'est certainement pas entier, car sa norme relative par rapport à $c(\zeta)$, c'est-à-dire $\frac{\alpha^l - \mu}{\lambda^l}$, est fractionnaire, à cause de $m < l$; donc, le nombre $\alpha - \mathsf{M}$

n'est pas divisible par $\mathfrak{l}$; par suite, l'idéal $\mathfrak{A}$ est différent de $\mathfrak{l}$. D'autre part, $\mathfrak{A}$ n'est égal à 1, car la norme relative du nombre $\alpha - \mathsf{M}$ est, à cause de

$$(71) \qquad N_k(\alpha - \mathsf{M}) = \alpha^l - \mathsf{M}^l = a\lambda^m, \quad (\mathfrak{l}^m)$$

divisible par $\mathfrak{l}^m$. Comme on a $S\mathfrak{A} = \mathfrak{A}$, $\mathfrak{A}$ est un idéal invariant, et comme ce doit être un facteur de $\mathfrak{l}$, ce dernier appartient à la première des trois catégories d'idéaux premiers du sous-corps distinguées (§ 57) dans la démonstration du théorème 93, c'est-à-dire $\mathfrak{l} = \mathfrak{L}^l$, $\mathfrak{L}$ étant un idéal premier, évidemment du premier degré de $c(\mathsf{M}, \zeta)$. La congruence (71) donne alors $\mathfrak{A} = \mathfrak{L}^m$.

Déterminons maintenant deux entiers positifs a et b, tels que $am - bl = 1$, et posons

$$\Omega = \frac{(\alpha - \mathsf{M})^a}{\lambda^b}.$$

De $S\mathsf{M} = \zeta\mathsf{M}$, on déduit

$$S\Omega = \frac{(\alpha - \mathsf{M} + \lambda\mathsf{M})^a}{\lambda^b}$$

et nous concluons de cette expression que $\Omega - S\Omega$ contient en facteur $\mathfrak{L}^{(l-m+1)}$. Comme il en est de même de toute différence entre Ω et un de ses conjugués, le discriminant relatif de Ω par rapport à $c(\zeta)$ contient en facteur exactement la $(l-1)(l-m+1)^{\text{ième}}$ puissance de l'idéal $\mathfrak{l}$. Il en résulte, Ω n'étant divisible que par la première puissance de $\mathfrak{L}$, que le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$ est aussi divisible par la même puissance (lemme 23).

Le discriminant relatif du corps kummerien $c(\mathsf{M}, \zeta)$ par rapport au corps $c(\zeta)$ est ainsi complètement défini, et l'on peut immédiatement en déduire le discriminant du corps $c(\mathsf{M}, \zeta)$ (théorème 39).

§ 127. — Le symbole $\left\{\frac{\mu}{\mathfrak{w}}\right\}$.

Il est nécessaire pour la suite de généraliser le symbole $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ introduit au paragraphe 113, pour le cas où μ est divisible par $\mathfrak{w}$ et pour celui où $\mathfrak{w} = \mathfrak{l}$.

Soit $\mathfrak{w}$ un idéal premier quelconque de $c(\zeta)$ et μ un entier quelconque de $c(\zeta)$, qui ne soit pas égal à la $l^{\text{ième}}$ puissance d'un entier de $c(\zeta)$. Quand le discriminant relatif du corps kummerien engendré par $\mathsf{M} = \sqrt[l]{\mu}$ et ζ sera divisible par $\mathfrak{w}$, le *symbole* $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ aura la valeur 0.

Si, au contraire, le discriminant relatif de ce corps $c(\mathsf{M}, \zeta)$ n'est pas divisible par $\mathfrak{w}$, on peut, d'après le théorème 148, toujours trouver dans $c(\zeta)$ un nombre α, tel que $\mu^* = \alpha^l\mu$, soit un entier de $c(\zeta)$ non divisible par $\mathfrak{w}$. Si μ est lui-même premier

à $\mathfrak{w}$, $\alpha = 1$ remplit déjà cette condition. Nous définissons alors, si $\mathfrak{w} \neq \mathfrak{l}$, le *symbole* en question par la formule

$$\left\{\frac{\mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^*}{\mathfrak{w}}\right\}.$$

Mais si $\mathfrak{w} = \mathfrak{l}$, on peut, le discriminant relatif de $c(\mathsf{M}, \zeta)$ devant être premier à $\mathfrak{l}$, choisir en outre le nombre α (théorème 148), de façon que l'on ait $\mu^* \equiv 1$, mod $\mathfrak{l}^l$. On a dès lors une congruence de la forme

$$\mu^* \equiv 1 + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

où a est un des nombres $0, 1, 2, \ldots l-1$. Je définis alors le *symbole* $\left\{\frac{\mu}{\mathfrak{l}}\right\}$ par l'égalité

$$\left\{\frac{\mu}{\mathfrak{l}}\right\} = \zeta^a.$$

Si μ est la $l^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$ et $\mathfrak{w}$ un idéal premier de $c(\zeta)$, on prendra $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$.

La valeur du symbole $\left\{\frac{\mu}{\mathfrak{w}}\right\}$ est ainsi fixée pour tout entier μ et tout idéal premier $\mathfrak{w}$ de $c(\zeta)$; elle est d'ailleurs égale à 0 ou à une racine $l^{\text{ième}}$ de l'unité.

Enfin $\mathfrak{a}$ étant un idéal quelconque du corps $c(\zeta)$, si l'on a $\mathfrak{a} = \mathfrak{p}\mathfrak{q} \ldots \mathfrak{w}$, $\mathfrak{p}$, $\mathfrak{q}$, etc. étant des idéaux premiers de $c(\zeta)$, on définira le *symbole* $\left\{\frac{\mu}{\mathfrak{a}}\right\}$ par l'égalité

$$\left\{\frac{\mu}{\mathfrak{a}}\right\} = \left\{\frac{\mu}{\mathfrak{p}}\right\}\left\{\frac{\mu}{\mathfrak{q}}\right\} \cdots \left\{\frac{\mu}{\mathfrak{w}}\right\},$$

$\mathfrak{a}$, $\mathfrak{b}$ étant des idéaux quelconques de $c(\zeta)$, on a donc

$$\left\{\frac{\mu}{\mathfrak{a}\mathfrak{b}}\right\} = \left\{\frac{\mu}{\mathfrak{a}}\right\}\left\{\frac{\mu}{\mathfrak{b}}\right\}.$$

§ 128. — Idéaux premiers d'un corps kummerien.

Soit μ un entier de $c(\zeta)$, $\mathsf{M} = \sqrt[l]{\mu}$ un nombre en dehors de $c(\zeta)$. La question de la décomposition des idéaux premiers du corps circulaire $c(\zeta)$ en idéaux premiers du corps kummerien $c(\mathsf{M}, \zeta)$ est résolue par le théorème suivant :

Théorème 149. — Un idéal premier quelconque $\mathfrak{p}$ de $c(\zeta)$ est, dans le corps kummerien $c(\mathsf{M}, \zeta)$, soit égal à la $l^{\text{ième}}$ puissance d'un idéal premier, soit décomposable en un produit de l idéaux premiers distincts, soit premier lui-même, selon que $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 0$, $= 1$ ou $=$ une racine $l^{\text{ième}}$ de l'unité différente de 1.

Démonstration. — La première partie de ce théorème se rapporte aux idéaux premiers qui divisent le discriminant relatif du corps kummerien : ils sont donc invariants, d'après le théorème 93. Ce fait ou le théorème 148 montrent donc pour ces idéaux l'exactitude du théorème.

Si $\mathfrak{p}$ est un idéal premier qui ne divise pas le discriminant relatif du corps $c(\mathsf{M}, \zeta)$, soit μ^* un entier non divisible par $\mathfrak{p}$, tel que le quotient $\frac{\mu^*}{\mu}$ soit égal à la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$. Le corps $c(\mathsf{M}, \zeta)$ est alors engendré également par $\mathsf{M}^* = \sqrt[l]{\mu^*}$ et ζ.

Examinons d'abord le cas de $\mathfrak{p} \neq \mathfrak{l}$. Si alors $\left(\frac{\mu^*}{\mathfrak{p}}\right) = 1$, le nombre μ^* est, d'après le théorème 139, résidu de $l^{\text{ème}}$ puissance, mod $\mathfrak{p}$. Déterminons, ce qui est toujours possible, un entier α de $c(\zeta)$, tel que l'on ait $\mu^* \equiv \alpha^l$, (mod $\mathfrak{p}$), et $\mu^* \not\equiv \alpha^l$, (mod $\mathfrak{p}^2$). En formant alors les idéaux conjugués relatifs

$$\begin{aligned} \mathfrak{P} &= (\mathfrak{p}, \mathsf{M}^* - \alpha), \\ S\mathfrak{P} &= (\mathfrak{p}, \zeta\mathsf{M}^* - \alpha), \\ &\dots\dots\dots \\ S^{l-1}\mathfrak{P} &= (\mathfrak{p}, \zeta^{l-1}\mathsf{M} - \alpha), \end{aligned}$$

nous obtenons facilement

$$\mathfrak{p} = \mathfrak{P}.S\mathfrak{P} \dots S^{l-1}\mathfrak{P}.$$

Comme

$$(\mathfrak{P}, S\mathfrak{P}) = (\mathfrak{p}, \mathsf{M}^* - \alpha, \zeta\mathsf{M} - \alpha) = 1,$$

$S\mathfrak{P}$ est différent de $\mathfrak{P}$, et, par suite, les l facteurs premiers $\mathfrak{P}$, $S\mathfrak{P}$, ... $S^{l-1}\mathfrak{P}$ de l'idéal $\mathfrak{p}$ sont distincts. L'idéal premier $\mathfrak{p}$ de $c(\zeta)$ appartient donc à la deuxième catégorie des idéaux premiers du sous-corps (théorème 93), il se décompose donc dans $c(\mathsf{M}, \zeta)$ en l idéaux premiers distincts. Inversement, si un idéal premier $\mathfrak{p}$ du corps $c(\zeta)$, différent ou non de l'idéal $\mathfrak{l}$, se décompose en l idéaux premiers distincts $\mathfrak{P}$, $S\mathfrak{P}$, ... $S^{l-1}\mathfrak{P}$ du corps $c(\mathsf{M}, \zeta)$, on a, p étant le nombre premier divisible par $\mathfrak{p}$, $N(\mathfrak{P}) = p^f$ et $N(\mathfrak{p}) = N(\mathfrak{P}) \dots N(S^{l-1}\mathfrak{P}) = p^{lf}$, et, par suite, la norme de $\mathfrak{p}$, prise dans le corps $c(\zeta)$, $n(\mathfrak{p})$ est aussi égale à p^f. L'égalité des normes $N(\mathfrak{P})$ et $n(\mathfrak{p})$ montre, comme au paragraphe 57, que tout entier du corps $c(\mathsf{M}, \zeta)$ est congru, mod $\mathfrak{P}$, à un entier du corps $c(\zeta)$; en posant en particulier $\mathsf{M}^* \equiv \alpha$, mod $\mathfrak{P}$, α étant dans $c(\zeta)$, on a $\mathsf{M}^{*l} = \mu^* \equiv \alpha^l$, mod $\mathfrak{P}$, et comme $\mu^* - \alpha^l$ est un nombre de $c(\zeta)$, on doit avoir aussi $\mu^* \equiv \alpha^l$, mod $\mathfrak{p}$, c'est-à-dire que $\left(\frac{\mu^*}{\mathfrak{p}}\right) = \left(\frac{\mu}{\mathfrak{p}}\right) = 1$. La dernière partie du théorème 149 est donc complètement démontrée pour le cas d'un idéal premier $\mathfrak{p} \neq \mathfrak{l}$.

Enfin, relativement à l'idéal premier $\mathfrak{l}$, si le discriminant relatif du corps $c(\mathsf{M}, \zeta)$

par rapport à $c(\zeta)$ n'est pas divisible par $\mathfrak{l}$, on a, pour le nombre μ^*, d'après le théorème 148, une congruence de la forme

$$\mu^* \equiv \alpha^l + a\lambda^l, \quad (\mathfrak{l}^{l+1}),$$

a étant un entier rationnel. Si maintenant l'on a $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$, c'est-à-dire si a est divisible par l, il en résulte une congruence de la forme

$$\mu^* \equiv \alpha^l + a^*\lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

où a^* est encore un entier rationnel. Si a^* n'est pas divisible par $\mathfrak{l}$, nous posons $\mu^{**} = \mu^*$; si, au contraire, a^* est divisible par l, nous posons

$$\mu^{**} = (1+\lambda)^l\mu^* = (1-\lambda^2)^l\mu;$$

il en résulte

$$\mu^{**} \equiv \alpha^l + \lambda^{l+1}\alpha^l, \quad (\mathfrak{l}^{l+2}).$$

D'après cela, le nombre μ^{**} vérifie toujours une congruence

$$\mu^{**} \equiv \alpha^l + a^{**}\lambda^{l+1}, \quad (\mathfrak{l}^{l+2}),$$

où a^{**} est un entier rationnel non divisible par l, et, par suite, en posant $\mathsf{M}^{**} = \sqrt[l]{\mu^{**}}$ et

$$\mathfrak{L} = \left(\lambda, \frac{\alpha - \mathsf{M}^{**}}{\lambda}\right),$$

on a la décomposition

$$\mathfrak{l} = \mathfrak{L}.S\mathfrak{L} \ldots S^{l-1}\mathfrak{L}.$$

Comme

$$\left(\lambda, \frac{\alpha - \mathsf{M}^{**}}{\lambda}, \frac{\alpha - \zeta\mathsf{M}^{**}}{\lambda}\right) = 1,$$

$S\mathfrak{L}$ est différent de $\mathfrak{L}$, et, par suite, les l idéaux premiers $\mathfrak{L}, S\mathfrak{L}, \ldots, S^{l-1}\mathfrak{L}$ sont distincts.

Inversement, si $\mathfrak{l}$ se décompose ainsi dans le corps kummerien, les normes de $\mathfrak{L}$ dans $c(\mathsf{M}, \zeta)$ et de $\mathfrak{l}$ dans $c(\zeta)$ sont égales, d'après une remarque antérieure, applicable, on l'a indiqué, même au cas de $\mathfrak{p} = \mathfrak{l}$, et, par suite, tout entier de $c(\mathsf{M}, \zeta)$ est congru mod $\mathfrak{L}$ à un entier de $c(\zeta)$. Comme ensuite, d'après le théorème 93, $\mathfrak{l}$ ne divise certainement pas le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$, nous pouvons, d'après le théorème 148, poser $\mu^* \equiv \alpha^l$, mod $\mathfrak{l}^l$, et $\frac{\alpha - \mathsf{M}^*}{\lambda}$ est donc un entier. Comme $\mathfrak{L}$ est un idéal premier du premier degré dans $c(\mathsf{M}, \zeta)$, nous pouvons trouver un entier rationnel a congru à cet entier mod $\mathfrak{L}$; alors on a, N_c désignant la norme relative par rapport à $c(\zeta)$,

$$N_c\left(\frac{\alpha - \mathsf{M}^*}{\lambda} - a\right) \equiv 0, \quad (\mathfrak{l}).$$

c'est-à-dire

$$(\alpha - a\lambda)^l - \mu^* \equiv 0, \quad (\mathfrak{l}^{l-1});$$

on a donc $\left(\frac{\mu^*}{\mathfrak{l}}\right) = \left(\frac{\mu}{\mathfrak{l}}\right) = 1$, ce qui achève la démonstration du théorème 149.

Le théorème 149 nous fournit un moyen simple de distinguer, dans le cas particulier des corps $c(\mathrm{M}, \zeta)$ et $c(\zeta)$, les trois sortes d'idéaux premiers indiquées au théorème 93 pour un corps supérieur cyclique relatif de degré relatif premier.

CHAPITRE XXIX.

Résidus et non résidus de normes d'un corps kummerien.

§ 129. — Définition des résidus de normes et des non résidus.

Soit, comme au paragraphe 125, μ un nombre de $c(\zeta)$, tel que $\mathrm{M} = \sqrt[l]{\mu}$ ne soit pas dans $c(\zeta)$ et soit $c(\mathrm{M}, \zeta)$ le corps kummerien déterminé par M et ζ; soit $\mathrm{N}_k(\mathrm{A})$ la norme relative d'un nombre A de $c(\mathrm{M}, \zeta)$ par rapport à $c(\zeta)$. Soit $\mathfrak{w}$ un idéal premier quelconque du corps circulaire $c(\zeta)$ et ν un entier quelconque de ce corps. Si alors ν est congru mod $\mathfrak{w}$ à la norme relative d'un entier de $c(\mathrm{M}, \zeta)$ et si, en outre, on peut trouver, pour une puissance de $\mathfrak{w}$ aussi élevée qu'on le veut, un entier A du corps $c(\mathrm{M}, \zeta)$, tel que l'on ait $\nu = \mathrm{N}_k(\mathrm{A})$ suivant cette puissance de $\mathfrak{w}$, j'appellerai ν *un résidu de normes du corps kummerien mod* $\mathfrak{w}$. Dans tout autre cas, ν sera *non résidu de normes du corps kummerien mod* $\mathfrak{w}$.

§ 130. — Théorème sur le nombre des résidus de normes. — Idéaux de ramification.

On a l'important théorème suivant :

Théorème 150. — *Si* $\mathfrak{w}$ *est un idéal premier du corps circulaire* $c(\zeta)$, *ne divisant pas le discriminant relatif du corps kummerien* $c(\mathrm{M}, \zeta)$, *tout entier de* $c(\zeta)$ *premier à* $\mathfrak{w}$ *est résidu de normes du corps kummerien mod* $\mathfrak{w}$.

Si, au contraire, $\mathfrak{w}$ *est un idéal premier du corps circulaire* $c(\zeta)$, *diviseur du discriminant relatif du corps kummerien* $c(\mathrm{M}, \zeta)$, *et qu'on désigne par e, dans le cas de* $\mathfrak{w} \neq \mathfrak{l}$, *un exposant positif quelconque, et, dans le cas de* $\mathfrak{w} = \mathfrak{l}$, *un exposant quelconque* $> l$, *il y a exactement un* $l^{\text{ième}}$ *de tous les nombres de* $c(\zeta)$ *premiers à* $\mathfrak{w}$ *et incongrus mod* $\mathfrak{w}^e$, *qui sont résidus de normes mod* $\mathfrak{w}$.

Démonstration. — Soit d'abord $\mathfrak{w}$ un idéal premier de $c(\zeta)$ différent de $\mathfrak{l}$ et ne divisant pas le discriminant relatif du corps $c(\mathsf{M}, \zeta)$; il y a deux cas à distinguer, suivant que $\mathfrak{w}$ est décomposable ou non dans $c(\mathsf{M}, \zeta)$. Dans le premier cas, soit $\mathfrak{W}$ un idéal premier facteur de $\mathfrak{w}$ dans $c(\mathsf{M}, \zeta)$. En nous reportant à la démonstration du théorème 148, nous pouvons, sans diminuer la généralité pour cela, admettre que μ, et par suite aussi le discriminant relatif du nombre $\mathsf{M} = \sqrt[l]{\mu}$ par rapport à $c(\zeta)$, ne sont pas divisibles par $\mathfrak{W}$; il y a dès lors certainement dans $c(\mathsf{M}, \zeta)$ un système de l entiers $\mathsf{A}_1, \ldots, \mathsf{A}_l$ vérifiant les congruences

$$\left.\begin{array}{l} \mathsf{A}_1 + \mathsf{A}_2\mathsf{M} + \ldots + \mathsf{A}_l\mathsf{M}^{l-1} \equiv \nu, \\ \mathsf{A}_1 + \mathsf{A}_2\zeta\mathsf{M} + \ldots + \mathsf{A}_l(\zeta\mathsf{M})^{l-1} \equiv 1, \\ \mathsf{A}_1 + \mathsf{A}_2\zeta^2\mathsf{M} + \ldots + \mathsf{A}_l(\zeta^2\mathsf{M})^{l-1} \equiv 1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \mathsf{A}_1 + \mathsf{A}_2\zeta^{l-1}\mathsf{M} + \ldots + \mathsf{A}_l(\zeta^{l-1}\mathsf{M})^{l-1} \equiv 1, \end{array}\right\} \quad (\mathfrak{W}).$$

Or, tout entier du corps $c(\mathsf{M}, \zeta)$ est évidemment congru mod $\mathfrak{W}$ à un entier de $c(\zeta)$; en posant

$$\mathsf{A}_1 \equiv \alpha_1, \quad \mathsf{A}_2 \equiv \alpha_2, \quad \ldots, \quad \mathsf{A}_l \equiv \alpha_l, \quad (\mathfrak{W}),$$

$\alpha_1, \alpha_2, \ldots, \alpha_l$ étant entiers dans $c(\zeta)$ et

$$\mathsf{A} \equiv \alpha_1 + \alpha_2\mathsf{M} + \ldots + \alpha_l\mathsf{M}^{l-1},$$

on en déduit

$$\nu \equiv \mathsf{A}, \quad 1 \equiv S\mathsf{A}, \quad \ldots, \quad 1 \equiv S^{l-1}\mathsf{A}, \quad (\mathfrak{W});$$

et en multipliant, on a $\nu \equiv N_c(\mathsf{A})$, mod $\mathfrak{W}$, et par suite aussi, mod $\mathfrak{w}$. Ceci démontre dans le cas présent la première partie du théorème pour le cas de $e = 1$. Pour passer aux cas de $e > 1$, supposons que l'on ait $\nu \not\equiv N_c(\mathsf{A})$, mod $\mathfrak{w}^2$, et posons alors

$$\frac{\nu}{N_c(\mathsf{A})} \equiv 1 + \omega, \quad (\mathfrak{w}^2),$$

ω étant un entier de $c(\zeta)$ divisible par $\mathfrak{w}$, mais non par $\mathfrak{w}^2$. L'entier $\mathsf{B} = \mathsf{A}(1 + l^*\omega)$, où l^* est un entier rationnel vérifiant la congruence $ll^* \equiv 1$, mod $\mathfrak{w}$ remplit alors la condition $\nu \equiv N_c(\mathsf{B})$, mod $\mathfrak{w}^2$. En continuant d'employer ce procédé, nous arrivons finalement, pour toute puissance $\mathfrak{w}^e$, à un entier de $c(\mathsf{M}, \zeta)$, dont la norme relative par rapport à $c(\zeta)$ est congrue à ν mod $\mathfrak{w}^e$.

Soit, d'autre part, $\mathfrak{w}$ indécomposable dans $c(\mathsf{M}, \zeta)$; nous pouvons encore supposer μ non divisible par $\mathfrak{w}$, et alors, d'après le théorème 149, μ n'est pas résidu de $l^{\text{ième}}$ puissance mod $\mathfrak{w}$. D'après les conséquences du théorème 139, il y a dans $c(\zeta)$ exactement $r = \dfrac{n(\mathfrak{w}) - 1}{l}$ résidus de $l^{\text{ième}}$ puissances mod $\mathfrak{w}$ premiers à $\mathfrak{w}$; en les représentant par $\rho_1, \ldots, \rho_r$, les $n(\mathfrak{w}) - 1$ nombres

$$\rho_i\mu^g \quad \begin{pmatrix} i = 1, 2, \ldots, r, \\ g = 0, 1, 2, \ldots, l-1 \end{pmatrix}$$

sont tous incongrus, mod $\mathfrak{w}$, car μ n'est pas résidu de $l^{\text{ième}}$ puissance, mod $\mathfrak{w}$, et, par suite, tout nombre de $c(\zeta)$ premier à $\mathfrak{w}$ est congru, mod $\mathfrak{w}$, à l'un de ces nombres. En posant $\rho_1 \equiv \alpha_1^l, \ldots, \rho_r \equiv \alpha_r^l$, mod $\mathfrak{w}$, $\alpha_1, \ldots, \alpha_r$ étant des nombres de $c(\zeta)$, on en déduit

$$\rho_r \mu^u \equiv \mathrm{N}_r(\alpha_r \mathsf{M}^u), \quad (\mathfrak{w}),$$

et, par suite, tout entier de $c(\zeta)$ premier à $\mathfrak{w}$ est congru mod $\mathfrak{w}$ à la norme relative d'un certain nombre de $c(\mathsf{M}, \zeta)$; on en conclut, comme dans le cas précédent, que pour tout nombre ν entier de $c(\zeta)$ premier à $\mathfrak{w}$, on peut trouver un entier de $c(\mathsf{M}, \zeta)$ dont la norme relative soit congrue à ν, mod $\mathfrak{w}^e$.

Si nous voulons maintenant démontrer la première partie du théorème 150 pour le cas de $\mathfrak{w} = \mathfrak{l}$, nous pouvons supposer μ premier à $\mathfrak{l}$; désignons par λ^m la plus haute puissance de λ contenue dans $\mu^{l-1} - 1$, m étant dans tous les cas ≥ 1, et posons

$$\mu^{l-1} \equiv 1 + a\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

a étant un entier rationnel premier à l; a^* étant alors un entier rationnel, tel que $aa^* \equiv -1$, mod l, en posant $u^* = \mu^{a^*(l-1)}$, on a

(72) $$\mu^* \equiv 1 - \lambda^m, \quad (\mathfrak{l}^{m+1}).$$

D'autre part, on a les congruences suivantes, où g est un entier positif quelconque et h un entier positif quelconque premier à l :

(73) $$\left.\begin{aligned} (1 - \lambda^{g+1})^l &\equiv 1 + \lambda^{l+g} \\ (1 - \lambda^{g+1})^{hl} &\equiv 1 + h\lambda^{l+g} \end{aligned}\right\}, \quad (\mathfrak{l}^{l+g+1}).$$

Comme le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$ ne peut, dans le cas actuel, contenir le facteur $\mathfrak{l}$, on a nécessairement, d'après le théorème 148, $m \geq l$ [1].

---

[1] N. T. — En effet, d'après le théorème 148, on doit avoir

$$\mu \equiv \alpha^l, \quad (\mathfrak{l}^l)$$

d'où

$$\mu^{l-1} \equiv \alpha^{l(l-1)}, \quad (\mathfrak{l}^l)$$

mais

$$\alpha^{l-1} \equiv 1, \quad (\mathfrak{l})$$

donc

$$\alpha^{l(l-1)} \equiv 1, \quad (\mathfrak{l}^l) \qquad \mu^{l-1} \equiv 1, \quad (\mathfrak{l}^l);$$

ainsi, dans

$$\mu^{l-1} \equiv 1 + a\lambda^m, \quad (\mathfrak{l}^{m+1})$$

on a

$$m \geq l.$$

Soit d'abord $m = l$. On déduit alors facilement (¹) des congruences (72) et (73) que pour tout entier positif g on peut trouver dans $c(\zeta)$ un entier α_g vérifiant la congruence

$$\mu^* \alpha_g^l \equiv 1 - \lambda^l + \lambda^{l+g}, \quad (\mathfrak{l}^{l+g+1}).$$

En posant alors $\mathsf{M} = \sqrt[l]{\mu^*}$ et $\Omega_g = \dfrac{1 - \alpha_g \mathsf{M}^*}{\lambda}$, Ω_g est toujours un entier de $c(\mathsf{M}, \zeta)$ et on a

$$N_c(\Omega_g) \equiv 1 - \lambda^g, \quad (\mathfrak{l}^{g+1}).$$

De là résulte immédiatement (²) que tout entier ν de $c(\zeta)$ vérifiant la congruence $\nu \equiv 1$, mod $\mathfrak{l}$, est résidu de normes du corps $c(\mathsf{M}, \zeta)$, mod $\mathfrak{l}$. On lève facilement cette

---

(¹) N. T. — On a

$$\mu^* \equiv 1 - \lambda^l, \quad (\mathfrak{l}^{l+1}).$$

Mais en multipliant μ^* par une série de puissances $l^{\text{ièmes}}$ convenables $(1 - \lambda^{r+1})^{ly}$, on peut avoir

$$\mu^* \prod (1 - \lambda^{r+1})^{ly} \equiv 1 - \lambda^l, \quad (\mathfrak{l}^{l+g+1}).$$

Soit, en effet,

$$\mu^* = 1 - \lambda^l + z\lambda^{l+k};$$

en multipliant membre à membre cette égalité et la congruence

$$(1 - \lambda^{r+1})^{ly} \equiv 1 + y\lambda^{l+r}, \quad (\mathfrak{l}^{l+r+1})$$

on obtient la congruence

$$\mu^*(1 - \lambda^{r+1})^{ly} \equiv 1 - \lambda^l + z\lambda^{l+k} + y\lambda^{l+r}, \quad (\mathfrak{l}^{l+r+1})$$

d'où en posant $r = k$ et $y \equiv -z$, $(\mathfrak{l})$

$$\mu^*(1 - \lambda^{k+1})^{ly} \equiv 1 - \lambda^{l}, \quad (\mathfrak{l}^{l+k+1}).$$

Posant alors

$$\mu^{**} = \mu^*(1 - \lambda^{k+1})^{ly} = 1 - \lambda^l + z^*\lambda^{l+k+1},$$

on aura de même

$$\mu^{**}(1 - \lambda^{k+2})^{ly} \equiv 1 - \lambda^l, \quad (\mathfrak{l}^{l+k+2})$$

et ainsi de suite, jusqu'à avoir

$$\mu^* \prod (1 - \lambda^{k+1})^{ly} \equiv 1 - \lambda^l, \quad (\mathfrak{l}^{l+g+1}).$$

Mais alors en multipliant membre à membre cette congruence et

$$(1 - \lambda^{g+1})^l \equiv 1 + \lambda^{l+g}, \quad (\mathfrak{l}^{l+g+1})$$

on aura

$$\mu^*(1 - \lambda^{g+1})^l \prod (1 - \lambda^{k+1})^{ly} \equiv 1 - \lambda^l + \lambda^{l+g}, \quad (\mathfrak{l}^{l+g+1})$$

$$\alpha_g = (1 - \lambda^{g+1}) \prod (1 - \lambda^{k+1})^{y}.$$

(²) N. T. — On a successivement

$$\nu = 1 = \zeta^l \equiv N_c(\zeta), \quad (\mathfrak{l})$$

$$\nu = 1 - a_1\lambda \equiv (1 - \lambda)^{a_1} \equiv N_c(\Omega_1^{a_1}), \quad (\mathfrak{l}^2)$$

$$\nu = 1 - a_1\lambda - a_2\lambda^2 \equiv N_c(\Omega_1^{a_1})(1 - b_1\lambda^2) \equiv N_c(\Omega_1^{a_1})(1 - \lambda^2)^{b_1} \equiv N_c(\Omega_1^{a_1}\Omega_2^{b_1}), \quad (\mathfrak{l}^3)$$

en posant

$$N_c(\Omega_1^{a_1}) \equiv 1 - a_1\lambda - a_2\lambda^2 + b_1\lambda^2, \quad (\mathfrak{l}^3)$$

et ainsi de suite.

restriction de $\nu \equiv 1$, mod $\mathfrak{l}$. En effet, ν étant un entier quelconque premier à $\mathfrak{l}$, congru mod $\mathfrak{l}$ à l'entier rationnel a, posons $\nu^* \equiv a^{*l}\nu$, a^* étant un entier tel que $aa^* \equiv 1$, mod $\mathfrak{l}$: alors on a évidemment $\nu^* \equiv 1$, mod $\mathfrak{l}$, et, d'autre part, ν et ν^* sont en même temps résidus ou non résidus de normes du corps $c(\mathsf{M}, \zeta)$, mod $\mathfrak{l}$.

Soit ensuite dans la formule (72) $m > l$, et, par suite, $\left(\frac{\mu}{\mathfrak{l}}\right) = 1$; nous pouvons alors, g étant un entier positif quelconque, trouver deux entiers α_g et α_{g+1} de $c(\zeta)$, tels que l'on ait

$$(74) \qquad \begin{cases} \mu^* \alpha_g^l \equiv 1 + \lambda^{l+1} + \lambda^{l+g+1}, & (\mathfrak{l}^{l+g+2}), \\ \mu^* \alpha_{g+1}^l \equiv 1 + \lambda^{l+1} + \lambda^{l+g+2}, & (\mathfrak{l}^{l+g+3}). \end{cases}$$

Nous posons, conformément au théorème 149, $\mathfrak{l} = \mathfrak{L}\mathfrak{L}' \ldots \mathfrak{L}^{(l-1)}$, $\mathfrak{L}, \mathfrak{L}', \ldots$ étant des idéaux premiers distincts du corps $c(\mathsf{M}, \zeta)$. Les deux nombres

$$\mathsf{A}_g = \frac{1 - \alpha_g \mathsf{M}^*}{\lambda}, \qquad \mathsf{A}_{g+1} = \frac{1 - \alpha_{g+1} \mathsf{M}^*}{\lambda},$$

où $\mathsf{M}^* = \sqrt[l]{\mu^*}$ sont des entiers, et comme l'on a $N_c(\mathsf{A}_g) \equiv -\lambda$, mod $\mathfrak{l}^2$, A_g est divisible par un des idéaux premiers facteurs de $\mathfrak{l}$, $\mathfrak{L}$ par exemple, et contient ce facteur au premier degré et aucun des autres. Des formules (74) résulte

$$\alpha_g^l \equiv \alpha_{g+1}^l, \quad (\mathfrak{l}^{l+2}),$$

et nous pouvons alors supposer que α_{g+1} soit choisi dans la série des nombres α_{g+1}, $\zeta\alpha_{g+1}, \ldots, \zeta^{l-1}\alpha_{g+1}$, de façon que l'on ait $\alpha_g \equiv \alpha_{g+1}$, mod $\mathfrak{l}^2$, et, par suite, $\mathsf{A}_g \equiv \mathsf{A}_{g+1}$, mod $\mathfrak{l}$. D'après la dernière de ces congruences, A_{g+1} est aussi divisible par $\mathfrak{L}$, mais non par $\mathfrak{L}', \ldots, \mathfrak{L}^{(l-1)}$; et comme on a aussi $N_c(\mathsf{A}_{g+1}) \equiv -\lambda$, mod $\mathfrak{l}^2$, A_{g+1} n'est divisible que par la première puissance de $\mathfrak{L}$. Nous pouvons, d'après ce qui a été déjà démontré, mettre le nombre fractionnaire $\frac{\mathsf{A}_g}{\mathsf{A}_{g+1}}$ sous forme d'une fraction dont les deux termes seront premiers à $\mathfrak{l}$. En posant $\frac{\mathsf{A}_g}{\mathsf{A}_{g+1}} \equiv \Omega_g$, mod $\mathfrak{l}^{g+1}$, de façon que Ω_g soit un entier de $c(\mathsf{M}, \zeta)$, on a

$$N_c(\Omega_g) \equiv \frac{N_c(\mathsf{A}_g)}{N_c(\mathsf{A}_{g+1})} \equiv 1 + \lambda^g, \quad (\mathfrak{l}^{g+1}).$$

Une telle formule étant possible pour tout exposant positif g, on montre comme plus haut que tout entier premier à $\mathfrak{l}$ est résidu de normes du corps $c(\mathsf{M}, \zeta)$.

Nous passons maintenant à la deuxième partie du théorème 150. Soit d'abord $\mathfrak{w}$ un idéal premier de $c(\zeta)$ différent de $\mathfrak{l}$, divisant le discriminant relatif de $c(\mathsf{M}, \zeta)$; nous avons alors, d'après le théorème 149, $\mathfrak{w} = \mathfrak{W}^l$, où $\mathfrak{W}$ est un idéal premier de $c(\mathsf{M}, \zeta)$. Tout entier de $c(\mathsf{M}, \zeta)$ doit alors être congru à un entier de $c(\zeta)$, mod $\mathfrak{W}$. Si alors un nombre donné ν de $c(\zeta)$ premier à $\mathfrak{w}$ doit être congru à la norme relative $N_c(\mathsf{A})$ d'un entier A de $c(\mathsf{M}, \zeta)$, et si nous posons $\mathsf{A} \equiv \alpha$, mod $\mathfrak{W}$, il en résulte nécessai-

rement $\nu \equiv \alpha^l$, mod $\mathfrak{W}$, et par suite, mod $\mathfrak{w}$, c'est-à-dire que ν est résidu de $l^{\text{ème}}$ puissance, mod $\mathfrak{w}$. Inversement, si un nombre ν de $c(\zeta)$ est résidu de $l^{\text{ième}}$ puissance, mod $\mathfrak{w}$, ν est aussi évidemment congru à une norme relative $N_c(\mathsf{A})$, mod $\mathfrak{w}$. Nous en concluons que les résidus de $l^{\text{èmes}}$ puissances, mod $\mathfrak{w}$, donnent aussi tous les résidus de normes, mod $\mathfrak{w}$ du corps $c(\mathsf{M}, \zeta)$.

Il reste enfin à traiter le cas, où $\mathfrak{w} = \mathfrak{l}$ et où $\mathfrak{l}$ divise le discriminant relatif de $c(\mathsf{M}, \zeta)$. On a dans ce cas $\mathfrak{l} = \mathfrak{L}^l$, $\mathfrak{L}$ étant idéal premier dans $c(\mathsf{M}, \zeta)$, et nous pouvons (vu le théorème 148) supposer que le nombre μ vérifie, soit la congruence

$$\mu \equiv \lambda, \quad (\mathfrak{l}^2),$$

soit l'une des suivantes

$$\mu \equiv 1 + \lambda^m, \quad (\mathfrak{l}^{m+1}),$$

m étant égal à $1, 2, \ldots, l-1$ (¹). Nous chercherons ensuite dans ces deux cas quels sont les nombres de $c(\zeta)$ qui sont congrus à la norme relative d'un nombre de $c(\mathsf{M}, \zeta)$, mod $\mathfrak{l}^{l-1}$ ou mod $\mathfrak{l}^l$ respectivement, et nous tirerons de là facilement le nombre des résidus de normes incongrus pour n'importe quelle puissance plus élevée de $\mathfrak{l}$.

Dans le cas de $\mu \equiv \lambda$, mod $\mathfrak{l}^2$, M est divisible par $\mathfrak{L}$, et non par $\mathfrak{L}^2$, et l'on a les congruences

$$(75)\quad \left\{\begin{array}{lll} & N_c(1+\mathsf{M}) \equiv 1+\lambda, & (\mathfrak{l}^2), \\ \text{c.-à-d.} & N_c(1+\mathsf{M}) \equiv 1+\lambda+\lambda^2\rho_1, & (\mathfrak{l}^{l+1}), \\ & N_c(1+\mathsf{M}^2) \equiv 1+\lambda^2, & (\mathfrak{l}^3), \\ \text{c.-à-d.} & N_c(1+\mathsf{M}^2) \equiv 1+\lambda^2+\lambda^3\rho_2, & (\mathfrak{l}^{l+1}), \\ & \cdots\cdots\cdots & \\ & N_c(1+\mathsf{M}^{l-1}) \equiv 1+\lambda^{l-1}, & (\mathfrak{l}^l), \\ \text{c.-à-d.} & N_c(1+\mathsf{M}^{l-1}) \equiv 1+\lambda^{l-1}+\lambda^l\rho_{l-1}, & (\mathfrak{l}^{l+1}), \end{array}\right.$$

où $\rho_1, \rho_2, \ldots, \rho_{l-1}$ sont des entiers de $c(\zeta)$.

(¹) N. T. — On a, en effet :

soit $\mu = \lambda^k\mu'$, k premier à l, μ' premier à λ ;

soit μ premier à λ et $\equiv \alpha^l$, $(\mathfrak{l}^m)$, $m < l$.

Dans le premier cas, on déterminera deux entiers a, b, tels que

$$ak + bl = 1,$$

et on prendra

$$\mu^* = \lambda^{bl}\mu^a = \lambda\mu'^a,$$

puis on déterminera μ'' de façon que $\mu''\mu' \equiv 1$, $(\mathfrak{l})$, et on prendra

$$\mu^{**} = \lambda\mu'^a\mu''^a \equiv \lambda, \quad (\mathfrak{l}^2).$$

Dans le deuxième cas, on déterminera β de façon que $\beta\alpha \equiv 1$, $(\mathfrak{l})$, d'où

$$\beta^l\mu \equiv 1 + a\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

et enfin on prendra $\mu^* = (\beta^l\mu)^{a^*}$, a^* vérifiant la congruence

$$a^*a \equiv 1, \quad (l).$$

Enfin, l'on a

(76) $$N_c(1+\lambda^t \mathsf{M}^u) \equiv 1, \quad (\mathfrak{l}^{l+1})$$

pour $t = 1, 2, 3, \ldots;\ u = 1, 2, \ldots, l-1$. Or, tout entier A du corps $c(\mathsf{M}, \zeta)$ premier à $\mathfrak{L}$ vérifie évidemment une congruence de la forme

$$\begin{aligned} \mathsf{A} \equiv a\,&(1+\mathsf{M})^{a_1}(1+\mathsf{M}^2)^{a_2}\ldots(1+\mathsf{M}^{l-1})^{a_{l-1}} \\ &(1+\lambda\mathsf{M})^{a'_1}(1+\lambda\mathsf{M}^2)^{a'_2}\ldots(1+\lambda\mathsf{M}^{l-1})^{a'_{l-1}} \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ &(1+\lambda^l\mathsf{M})^{a^{(l)}_1}(1+\lambda^l\mathsf{M}^2)^{a^{(l)}_2}\ldots(1+\lambda^l\mathsf{M}^{l-1})^{a^{(l)}_{l-1}}, \quad (\mathfrak{L}^{l^2}), \end{aligned}$$

où a est l'un des nombres $1, 2, \ldots, l-1$ et les $(l+1)(l-1)$ exposants a_1, $a_2, \ldots, a^{(l)}_{l-1}$ sont des entiers déterminés de la suite $0, 1, 2, \ldots, l-1$. Des congruences (75) et (76) résulte

$$N_c(\mathsf{A}) \equiv a^l(1+\lambda+\lambda^2\rho_1)^{a_1}(1+\lambda^2+\lambda^3\rho_2)^{a_2}\ldots(1+\lambda^{l-1}+\lambda^l\rho_{l-1})^{a_{l-1}}, \quad (\mathfrak{l}^{l+1}).$$

L'expression du second membre représente, lorsque a prend les valeurs $1, 2, \ldots, l-1$ et $a_1, a_2, \ldots, a_{l-1}$ séparément, toutes les valeurs $0, 1, 2, \ldots, l-1$, $(l-1)l^{l-1}$ nombres, visiblement incongrus mod $\mathfrak{l}^{l+1}$. Alors tout nombre de $c(\zeta)$ premier à $\mathfrak{l}$, congru mod $\mathfrak{l}^{l+1}$ à la norme relative $N_c(\mathsf{A})$ d'un nombre A de $c(\mathsf{M}, \zeta)$ est nécessairement congru mod $\mathfrak{l}^{l+1}$ à une expression de cette forme et inversement, on conclut de (75) que toute expression de cette forme est congrue mod $\mathfrak{l}^{l+1}$ à la norme relative d'un nombre de $c(\mathsf{M}, \zeta)$. A l'aide des congruences (73) on reconnaît que deux nombres de $c(\zeta)$ premiers à $\mathfrak{l}$, congrus mod $\mathfrak{l}^{l+1}$, sont en même temps résidus ou non résidus de normes mod $\mathfrak{l}$. Le nombre des résidus de normes mod $\mathfrak{l}$, premiers à $\mathfrak{l}$ et incongrus mod $\mathfrak{l}^{l+1}$ est donc exactement égal à $(l-1)l^{l-1}$, c'est-à-dire au $l^{\text{ième}}$ des nombres de $c(\zeta)$ premiers à $\mathfrak{l}$ et incongrus mod $\mathfrak{l}^{l+1}$, et ce résultat peut s'étendre immédiatement aux puissances $\mathfrak{l}^e$ d'exposant $e > l+1$.

Pour abréger, nous ne traiterons ici que le cas le plus simple de ceux qui sont encore possibles relativement à μ ; c'est celui de $\mu \equiv 1+\lambda$, mod $\mathfrak{l}^2$. En posant alors $\Omega = \mathsf{M} - 1$, Ω est un entier de $c(\mathsf{M}, \zeta)$ divisible par $\mathfrak{L}$, mais non par $\mathfrak{L}^2$, et en remarquant que $N_c(\Omega) \equiv \lambda$, mod $\mathfrak{l}^2$, on trouve, par un calcul facile (¹), les

---

(¹) N. T. — $N_c(1+\Omega^t)$ est égal à $-f_t(-1)$, si l'on représente par $f_t(x) = 0$ l'équation, de premier coefficient égal à 1, dont les racines sont $+\Omega^t$, $+(s\Omega)^t$, etc. Or, cette équation est la transformée de l'équation $f_1(y) = 0$ par la substitution $x = +y^t$. On a $f_1(y) = (y+1)^l - \mu$, et on en déduit que

$$f_t(x) = x^l + l\varphi(x) - (\mu-1)^t,$$

d'où

$$-f_t(-1) \equiv 1 + \lambda^t, \quad (\mathfrak{l}^{l+1}).$$

congruences

$$
(77)\quad
\begin{cases}
N_c(1+\Omega) \equiv 1+\lambda, & (\mathfrak{L}^2),\\
\text{c.-à-d. } N_c(1+\Omega) \equiv 1+\lambda+\lambda^2\rho_1, & (\mathfrak{L}^l),\\
N_c(1+\Omega^2) \equiv 1+\lambda^2, & (\mathfrak{L}^3),\\
\text{c.-à-d. } N_c(1+\Omega^2) \equiv 1+\lambda^2+\lambda^3\rho_2, & (\mathfrak{L}^l),\\
\dots\dots\dots\dots\dots\dots & \\
N_c(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}, & (\mathfrak{L}^{l-1}),\\
\text{c.-à-d. } N_c(1+\Omega^{l-2}) \equiv 1+\lambda^{l-2}+\lambda^{l-1}\rho_{l-2}, & (\mathfrak{L}^l),
\end{cases}
$$

où $\rho_1, \rho_2, \dots, \rho_{l-2}$ sont des entiers de $c(\zeta)$. On a de plus

$$N_c(1+\Omega^{l-1}) = 1+\Sigma_1+\Sigma_2+\dots+\Sigma_{l-1}+N_c(\Omega^{l-1})$$

en posant pour abréger

$$\Sigma_1 = \Omega^{l-1}+(S\Omega)^{l-1}+\dots+(S^{l-1}\Omega)^{l-1},$$
$$\Sigma_2 = \Omega^{l-1}(S\Omega)^{l-1}+\Omega^{l-1}(S^2\Omega)^{l-1}+\dots+(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\Sigma_3 = \Omega^{l-1}(S\Omega)^{l-1}(S^2\Omega)^{l-1}+\dots+(S^{l-3}\Omega)^{l-1}(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$

On a de suite $\Sigma_1 \equiv l$. Chacun des termes à additionner dans $\Sigma_2, \Sigma_3, \dots, \Sigma_{l-1}$ est divisible par $\mathfrak{L}^l$, on peut de plus les grouper en l séries, se déduisant l'une de l'autre par les substitutions $1, S, S^2, \dots, S^{l-1}$; en mettant alors un terme quelconque sous la forme $\lambda\Phi$, Φ est un entier de $c(\mathbf{M}, \zeta)$, et peut, par suite (démonstration du lemme 23), se mettre sous la forme d'un polynôme entier en Ω et par suite aussi en $\mathbf{M}$, dont les coefficients sont des entiers ou des fractions de $c(\zeta)$ à dénominateurs toujours premiers à $\mathfrak{l}$. En posant donc $\Phi = F(\mathbf{M})$, l'ensemble des l sommes peut s'écrire

$$\lambda\{F(\mathbf{M})+F(\zeta\mathbf{M})+\dots+F(\zeta^{l-1}\mathbf{M})\},$$

la parenthèse est, on le voit aisément, toujours congrue à 0, mod l; les nombres $\Sigma_2, \Sigma_3, \dots, \Sigma_{l-1}$ sont donc tous congrus à 0, mod $\mathfrak{L}^l$, et l'on a

$$(78)\qquad N_c(1+\Omega^{l-1}) \equiv 1+l+\lambda^{l-1} \equiv 1, \quad (\mathfrak{L}^l).$$

On obtient enfin facilement les congruences

$$(79)\qquad N_c(1+\lambda^g\Omega^h) \equiv 1, \quad (\mathfrak{L}^l),$$

pour $h = 1, 2, \dots, l-1$; $g = 1, 2, \dots, l-1$.

Maintenant tout entier de $c(\mathbf{M}, \zeta)$ premier à $\mathfrak{L}$ vérifie évidemment une congruence de la forme

$$
\begin{aligned}
A \equiv a(1+\Omega)^{n_1} & (1+\Omega^2)^{n_2} \dots (1+\Omega^{l-1})^{n_{l-1}}\\
(1+\lambda\Omega)^{n'_1} & (1+\lambda\Omega^2)^{n'_2} \dots (1+\lambda\Omega^{l-1})^{n'_{l-1}}\\
\dots\dots & \dots\dots\dots\dots\\
(1+\lambda^{l-1}\Omega)^{n_1^{(l-1)}} & (1+\lambda^{l-1}\Omega^2)^{n_2^{(l-1)}} \dots (1+\lambda^{l-1}\Omega^{l-1})^{n_{l-1}^{(l-1)}}, \quad (\mathfrak{L}^l).
\end{aligned}
$$

où a est un des nombres $1, 2, \dots, l-1$ et où les $l-2$ exposants $a_1, a_2, \dots, a_{l-2}$ sont des nombres déterminés de la suite $0, 1, 2, \dots, l-1$. On en déduit, vu les congruences (77), (78), (79),

$$N_c(\mathsf{A}) \equiv a^l(1+\lambda+\lambda^2\rho_1)^{a_1}(1+\lambda^2+\lambda^3\rho_2)^{a_2}\dots(1+\lambda^{l-2}+\lambda^{l-1}\rho_{l-2})^{a_{l-2}}, \quad (\mathfrak{l}^l).$$

Le second membre représente alors pour les $l-1$ valeurs $1, 2, \dots, l-1$ de a et les l valeurs $0, 1, 2, \dots, l-1$ des exposants $a_1, a_2, \dots, a_{l-2}$, $(l-1)l^{l-2}$ nombres, qui sont premiers à $\mathfrak{l}$ et incongrus mod $\mathfrak{l}^l$. A l'aide de la congruence $N_c(1+\lambda^l\mathsf{M}) \equiv 1+\lambda^l$, mod $\mathfrak{l}^{l+1}$ et des congruences (73), nous en concluons que le $l^{\text{ième}}$ de tous les nombres premiers à $\mathfrak{l}$ et incongrus mod $\mathfrak{l}^l$ donne tous les résidus de normes de $c(\mathsf{M}, \zeta)$, et nous étendons ensuite ce résultat au cas des puissances $\mathfrak{l}^e$ à exposant $e = l+1$ ou $> l+1$.

On obtient le même résultat par des calculs analogues lorsque μ est $\equiv 1$, mod $\mathfrak{l}^2$, et le théorème 150 est ainsi complètement démontré. Remarquons pourtant que nous nous arrangerons dans ce qui suit pour n'employer ce théorème que dans le cas $\mu \equiv 1+\lambda$, mod $\mathfrak{l}^2$, dont nous avons fait la démonstration en détail.

Le théorème 150 conduit à une propriété nouvelle et essentielle des idéaux premiers facteurs du discriminant relatif de $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$. Cette propriété correspond dans une certaine mesure au théorème sur les points de ramification d'une surface de Riemann, d'après lequel une fonction algébrique a dans le voisinage d'un point de ramification du $l^{\text{ième}}$ ordre une représentation conforme de l'angle total sur le $l^{\text{ième}}$ de ce dernier. Pour cette raison, j'appelle les facteurs idéaux premiers $\mathfrak{w}$ du discriminant relatif de $c(\mathsf{M}, \zeta)$ par rapport à $c(\zeta)$ des *idéaux de ramification* pour le corps de $c(\mathsf{M}, \zeta)$; « facteur premier du discriminant relatif », « idéal invariant », « idéal de ramification » sont donc ici synonymes.

§ 131. — Le symbole $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$.

Le théorème 150 nous fait voir la possibilité de répartir les nombres du corps $c(\zeta)$ incongrus mod $\mathfrak{w}^e$ ($e > l$ dans le cas de $\mathfrak{w} = \mathfrak{l}$) en l sections, contenant toutes le même nombre de nombres et dont l'une comprend les résidus des normes mod $\mathfrak{w}$. Pour mettre en lumière cette répartition, j'introduis un nouveau symbole $\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$, faisant correspondre comme suit une racine $l^{\text{ième}}$ déterminée de l'unité à deux entiers distincts ν et μ de $c(\zeta)$ et à un idéal premier $\mathfrak{w}$ quelconque de ce corps.

Soit d'abord $\mathfrak{w} \neq \mathfrak{l}$. Alors si ν est divisible exactement par $\mathfrak{w}^b$ et μ par $\mathfrak{w}^a$, on formera le nombre $\varkappa = \frac{\nu^a}{\mu^b}$ et on mettra $\varkappa$ sous forme d'une fraction $\frac{\rho}{\sigma}$ dont les deux

termes seront premiers à $\mathfrak{w}$. Le *symbole* $\left\{\frac{\nu,\,\mu}{\mathfrak{w}}\right\}$ sera alors défini par la formule

$$\left\{\frac{\nu,\,\mu}{\mathfrak{w}}\right\}=\left\{\frac{\varkappa}{\mathfrak{w}}\right\}=\left\{\frac{\rho}{\mathfrak{w}}\right\}\left\{\frac{\sigma}{\mathfrak{w}}\right\}^{-1}.$$

On obtient immédiatement les règles simples

$$(80)\qquad\left\{\begin{aligned}&\left\{\frac{\nu_1\nu_2,\,\mu}{\mathfrak{w}}\right\}=\left\{\frac{\nu_1,\,\mu}{\mathfrak{w}}\right\}\left\{\frac{\nu_2,\,\mu}{\mathfrak{w}}\right\}\\&\left\{\frac{\nu,\,\mu_1\mu_2}{\mathfrak{w}}\right\}=\left\{\frac{\nu,\,\mu_1}{\mathfrak{w}}\right\}\left\{\frac{\nu,\,\mu_2}{\mathfrak{w}}\right\}\\&\left\{\frac{\nu,\,\mu}{\mathfrak{w}}\right\}\left\{\frac{\mu,\,\nu}{\mathfrak{w}}\right\}=1,\end{aligned}\right.$$

où $\nu, \nu_1, \nu_2, \mu, \mu_1, \mu_2$ sont des entiers quelconques $\neq 0$ de $c(\zeta)$.

Pour définir le nouveau symbole dans le cas de $\mathfrak{w}=\mathfrak{l}$, faisons les remarques suivantes :

Etant donné un entier ω de $c(\zeta)$ vérifiant la congruence $\omega\equiv 1$, mod $\mathfrak{l}$, et si l'on pose

$$\omega=c+c_1\zeta+\ldots+c_{l-2}\zeta^{l-2},$$

de façon que $c, c_1, \ldots, c_{l-2}$ soient des entiers rationnels, ces derniers vérifient la congruence

$$c+c_1+\ldots+c_{l-2}\equiv 1,\quad(\mathrm{mod}\ l).$$

En posant alors

$$\omega(x)=c+c_1x+\ldots+c_{l-2}x^{l-2}-\frac{c+c_1+\ldots+c_{l-2}-1}{l}(1+x+\ldots+x^{l-1}),$$

$\omega(x)$ représente un polynôme à coefficients entiers de degré $l-1$ et l'on a

$$\omega(1)=1,\qquad\omega(\zeta)=\omega.$$

Ce polynôme s'appellera le *polynôme adjoint à l'entier* ω. Nous écrirons encore

$$\left[\frac{d^q\log\omega(e^v)}{dv^q}\right]_{v=0}=l^{(q)}(\omega),\qquad(q=1,2,\ldots,l-1)$$

expressions introduites avantageusement par Kummer pour abréger certains calculs. [Kummer[12].]

Si le nombre $\omega\equiv 1$, mod $\mathfrak{l}$, est mis d'une façon quelconque sous la forme

$$\omega=a+a_1\zeta+\ldots+a_l\zeta^l,$$

où $a, a_1, \ldots, a_l$ sont des entiers rationnels,

$$\bar{\omega}(x)=a+a_1x+\ldots+a_lx^l$$

est un polynôme de degré l, ne vérifiant pas en général l'égalité $\omega(1)=1$, mais véri-

fiant toujours la congruence $\varpi(1) \equiv 1$, mod l, et qui est par suite premier à l pour $x = 1$. On a les congruences suivantes :

(81)′
$$\left[\frac{d^q \log \varpi(e^v)}{dv^q}\right]_{v=0} \equiv l^{q}(\omega), \quad (\text{mod } l), \qquad (q = 1, 2, \ldots, l-2)$$

$$\left[\frac{d^{l-1} \log \varpi(e^v)}{dv^{l-1}}\right]_{v=0} \equiv l^{l-1}(\omega) + \frac{1-\varpi(1)}{l}, \quad (\text{mod } l).$$

Leur exactitude ressort de ce que l'on a

(81)″
$$\omega(x) = \varpi(x) + \frac{1-\varpi(1)}{l}(1 + x + \ldots + x^{l-1}) + O(x)(x^l - 1),$$

$$\omega(e^v) \equiv \varpi(e^v) + \frac{1-\varpi(1)}{l} v^{l-1}, \qquad (\text{mod } l).$$

Dans la première égalité, $O(x)$ désigne un certain polynôme entier en x, et la seconde signifie que, dans les développements des deux membres de cette congruence suivant les puissances de v, les coefficients de $1, v, v^2, \ldots, v^{l-1}$ sont congrus entre eux mod l (¹).

ν, μ étant deux entiers quelconques de $c(\zeta)$, tels que $\nu \equiv 1$, $\mu \equiv 1$, mod $\mathfrak{l}$, nous définissons le *symbole* $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ comme suit :

(82)
$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{l^{(1)}(\nu) l^{(l-1)}(\mu) - l^{(2)}(\nu) l^{(l-2)}(\mu) + \ldots - l^{(l-1)}(\nu) l^{(1)}(\mu)}.$$

(¹) N. T. — Soit, plus généralement, $\omega(\zeta)$ un entier de $c(\zeta)$ non divisible par $\mathfrak{l}$, de sorte que $\omega(1)$ ne soit pas divisible par l, et soit $\omega^*(\zeta)$ le même nombre exprimé d'une autre façon ; on aura encore

$$\left[\frac{d^q \log \omega(e^v)}{dv^q}\right]_{v=0} \equiv \left[\frac{d^q \log \omega^*(e^v)}{dv^q}\right]_{v=0}, \quad (\text{mod } l),$$
pour $q = 1, 2, \ldots, l-2$.

En effet, soit

$$\Omega(\zeta) = a_0 + a_1\zeta + \ldots + a_{l-2}\zeta^{l-2}$$

la forme réduite de $\omega(\zeta)$ et de $\omega^*(\zeta)$, de sorte que l'on ait

$$\omega(x) = (1 + x + \ldots + x^{l-1})Q(x) + \Omega(x),$$
$$\omega^*(x) = (1 + x + \ldots + x^{l-1})Q^*(x) + \Omega(x).$$

$1 + x + \ldots + x^{l-1}$ et ses $l-2$ premières dérivées sont divisibles par l pour $x = 1$ (à cause de la congruence $1 + x + \ldots + x^{l-1} \equiv (1-x)^{l-1}$, mod l).

$\omega(e^v)$, $\omega^*(e^v)$, $\Omega(e^v)$ sont donc congrus entre eux, mod l, ainsi que leurs $l-2$ premières dérivées, et il en est par suite de même des dérivées logarithmiques.

Si deux nombres $\alpha(\zeta)$, $\beta(\zeta)$ sont congrus, mod l, on a évidemment aussi pour toute valeur de q

$$\left[\frac{d^q \log \alpha(e^v)}{dv^q}\right]_{v=0} \equiv \left[\frac{d^q \log \beta(e^v)}{dv^q}\right]_{v=0}, \quad (\text{mod } l).$$

De cette définition découlent immédiatement les règles

$$(83)\quad \begin{cases} \left(\dfrac{\nu_1\nu_2,\ \mu}{\mathfrak{l}}\right)=\left(\dfrac{\nu_1,\ \mu}{\mathfrak{l}}\right)\left(\dfrac{\nu_2,\ \mu}{\mathfrak{l}}\right), \\[2ex] \left(\dfrac{\nu,\ \mu_1\mu_2}{\mathfrak{l}}\right)=\left(\dfrac{\nu,\ \mu_1}{\mathfrak{l}}\right)\left(\dfrac{\nu,\ \mu_2}{\mathfrak{l}}\right), \\[2ex] \left(\dfrac{\nu,\ \mu}{\mathfrak{l}}\right)\left(\dfrac{\mu,\ \nu}{\mathfrak{l}}\right)=1, \end{cases}$$

où ν, ν_1, ν_2, μ, μ_1, μ_2 désignent des entiers quelconques de $c(\zeta)\equiv 1$, mod $\mathfrak{l}$. Si r est une racine primitive, mod l, et $s=(\zeta:\zeta^r)$ la substitution correspondante du corps circulaire $c(\zeta)$, on trouve aisément la formule

$$(84)\quad \left(\frac{s\nu,\ s\mu}{\mathfrak{l}}\right)=\left(\frac{\nu,\ \mu}{\mathfrak{l}}\right)^r.$$

Si ν et μ sont des entiers quelconques premiers à $\mathfrak{l}$ du corps $c(\zeta)$, je définirai le *symbole* $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ par la formule

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}=\left(\frac{\nu^{l-1},\ \mu^{l-1}}{\mathfrak{l}}\right).$$

Dans le cas où l'un des nombres ν, μ ou tous les deux sont divisibles par $\mathfrak{l}$, voir les remarques à la fin du paragraphe 133.

§ 132. — Lemmes sur le symbole $\left(\frac{\nu,\ \mu}{\mathfrak{l}}\right)$ et les résidus de normes mod $\mathfrak{l}$.

Lemme 24. — ω étant un entier de $c(\zeta)$ congru à 1, mod $\mathfrak{l}$, la norme $n(\omega)$ de ω dans $c(\zeta)$ vérifie la congruence

$$l^{(l-1)}(\omega)\equiv\frac{1-n(\omega)}{l}, \qquad (\text{mod } l).$$

[Kummer[20].]

Démonstration. — Soit $\omega(x)$ le polynôme adjoint à ω, et soit

$$F(x)=\prod_{(g)}\omega(1+x(\zeta^g-1)),$$

le produit étant étendu aux valeurs $g=0, 1, \ldots, l-1$. $F(x)$ est un polynôme en x à coefficients entiers et les coefficients de tous les termes divisibles par x^l sont évi-

demment divisibles par λ^l, et par suite aussi, à cause de la rationalité des coefficients, par l^2. En développant suivant les puissances de x, on obtient ensuite

$$(85)\quad \begin{cases} \log \omega(1+x(\zeta-1)) = \dfrac{\zeta-1}{1!}\, x \left[\dfrac{d \log \omega(x)}{dx}\right]_{x=1} \\ \quad + \dfrac{(\zeta-1)^2}{2!}\, x^2 \left[\dfrac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} + \ldots \\ \quad + \dfrac{(\zeta-1)^{l-1}}{(l-1)!}\, x^{l-1} \left[\dfrac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1} + \ldots. \end{cases}$$

En posant successivement dans ce développement $\zeta = 1, \zeta, \zeta^2, \ldots, \zeta^{l-1}$ et ajoutant, on obtient, vu

$$(\zeta-1)^g + (\zeta^2-1)^g + \ldots + (\zeta^{l-1}-1)^g = (-1)^g l, \qquad (g = 1, 2, \ldots, l-1)$$

l'égalité

$$(86)\quad \begin{cases} \log F(x) = l \Big\{ -\dfrac{x}{1!}\left[\dfrac{d \log \omega(x)}{dx}\right]_{x=1} + \dfrac{x^2}{2!}\left[\dfrac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} - \ldots \\ \quad + \dfrac{x^{l-1}}{(l-1)!}\left[\dfrac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1} \Big\} + x^l G, \end{cases}$$

où $x^l G$ représente l'ensemble des termes du développement divisibles par x^l.

En posant, en second lieu, dans le développement (85), $\zeta = e^v$ et prenant la $(l-1)^{\text{ième}}$ dérivée par rapport à v, celle-ci est égale, pour $v = 0$, à

$$(87)\quad \begin{cases} \left[\dfrac{d^{l-1} \log \omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0} = \dfrac{x}{1!}\left[\dfrac{d \log \omega(x)}{dx}\right]_{x=1} \\ \quad + \dfrac{2^{l-1} - 2\,.\,1^{l-1}}{2!}\, x^2 \left[\dfrac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} \\ \quad + \dfrac{3^{l-1} - 3\,.\,2^{l-1} + 3\,.\,1^{l-1}}{3!}\, x^3 \left[\dfrac{d^3 \log \omega(x)}{dx^3}\right]_{x=1} + \ldots \\ \quad + \dfrac{(l-1)^{l-1} - \ldots - (l-1)1^{l-1}}{(l-1)!}\, x^{l-1} \left[\dfrac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1} \\ \quad \equiv \dfrac{x}{1!}\left[\dfrac{d \log \omega(x)}{dx}\right]_{x=1} - \dfrac{x^2}{2!}\left[\dfrac{d^2 \log \omega(x)}{dx^2}\right]_{x=1} + \ldots \\ \quad - \dfrac{x^{l-1}}{(l-1)!}\left[\dfrac{d^{l-1} \log \omega(x)}{dx^{l-1}}\right]_{x=1}, \quad (\text{mod } l). \end{cases}$$

En comparant les formules (86) et (87), on obtient

$$\log F(x) \equiv -l \left[\frac{d^{l-1} \log \omega(1+x(e^v-1))}{dv^{l-1}}\right]_{v=0}, \qquad (\text{mod } l^2),$$

c'est-à-dire que les coefficients de $x, x^2, \ldots, x^{l-1}$ dans le premier membre sont congrus mod l^2 aux coefficients correspondants du second membre, et si nous passons

aux puissances de e nous obtenons, d'abord dans le même sens, puis, vu la remarque faite au début de cette démonstration, sans restriction, la congruence des deux polynômes à coefficients entiers

$$F(x) \equiv 1 - l\left[\frac{d^{l-1}\log\omega(1 + x(e^{v} - 1))}{dv^{l-1}}\right]_{v=0}, \quad (\text{mod } l^2),$$

et par suite, pour $x = 1$,

$$n(\omega) \equiv 1 - l.l^{(l-1)}(\omega), \quad (\text{mod } l^2),$$

ce qui démontre le lemme 24.

Lemme 25. — Si les entiers ν, μ de $c(\zeta)$ vérifient les congruences $\nu \equiv 1$, mod $\mathfrak{l}$, et $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}$, et si de plus ν est congru mod $\mathfrak{l}^l$ à la norme relative d'un entier A du corps kummerien $c(\mathsf{M}, \zeta)$ défini par $\mathsf{M} = \sqrt[l]{\mu}$, il existe un polynôme $f(x)$ de degré $l - 1$ à coefficients entiers, tel que l'on a

$$f(1) > 0,$$
$$n(f(\zeta)) \equiv 1, \quad (\text{mod } l^2),$$
$$\nu \equiv f(\mu), \quad (\text{mod } \mathfrak{l}^l).$$ [Kummer [20].]

Démonstration. — Vu la démonstration du lemme 23, tout entier A de $c(\mathsf{M}, \zeta)$ peut être mis sous la forme

$$\mathsf{A} = \frac{\gamma + \gamma_1(\mathsf{M} - 1) + \ldots + \gamma_{l-1}(\mathsf{M} - 1)^{l-1}}{\delta},$$

et par suite aussi sous la forme

$$\mathsf{A} = \frac{\beta + \beta_1\mathsf{M} + \ldots + \beta_{l-1}\mathsf{M}^{l-1}}{\delta},$$

$\gamma, \gamma_1, \ldots, \gamma_{l-1}, \delta, \beta, \beta_1, \ldots, \beta_{l-1}$ étant des entiers de $c(\zeta)$, δ premier à $\mathfrak{l}$. Ce dernier fait entraîne

$$\mathsf{A} \equiv \alpha + \alpha_1\mathsf{M} + \ldots + \alpha_{l-1}\mathsf{M}^{l-1}, \quad (\mathfrak{l}^l),$$

$\alpha, \alpha_1, \ldots, \alpha_{l-1}$ étant des entiers de $c(\zeta)$.

Soient alors

$$\alpha \equiv a^*, \ \alpha_1 \equiv a^*_1, \ \ldots, \ \alpha_{l-1} \equiv a^*_{l-1}, \quad (\text{mod } \mathfrak{l}),$$

$a^*, a^*_1, \ldots$ étant des entiers positifs; posons

$$f^*(x) = a^* + a^*_1 x + \ldots + a^*_{l-1}x^{l-1}.$$

Comme on a, dans $c(\mathsf{M}, \zeta)$, $\mathfrak{l} = \mathfrak{L}^l$ et $\mathsf{M} \equiv 1$, mod $\mathfrak{L}$, il en résulte

$$\mathsf{A} \equiv \alpha + \alpha_1 + \ldots + \alpha_{l-1} \equiv a^* + a^*_1 + \ldots + a^*_{l-1}, \quad (\text{mod } \mathfrak{L}).$$

Si maintenant on a, selon l'hypothèse de l'énoncé, $N(\mathsf{A}) \equiv \nu$, mod $\mathfrak{l}$, on a de plus

$$\nu \equiv N_k(\mathsf{A}) \equiv a + a_1 + \ldots + a_{l-1} \equiv 1, \quad (\text{mod } \mathfrak{L}),$$

et par suite

(88) $$a + a_1 + \ldots + a_{l-1} \equiv 1, \quad (\text{mod } l).$$

Par suite, $f^*(\zeta)$ est un nombre de $c(\zeta)$ congru à 1, mod $\mathfrak{l}$. On trouve alors aisément un entier positif b, tel que la norme du nombre $f(\zeta) = f^*(\zeta) + lb$ dans $c(\zeta)$ vérifie la congruence

(89) $$n(f(\zeta)) \equiv 1, \quad (\text{mod } l^2),$$

le polynôme entier

$$f(x) = f^*(x) + lb = a + a_1 x + \ldots + a_{l-1} x^{l-1}$$

remplit alors les conditions du lemme 25. Car on a évidemment $\mathsf{A} = f(\mathsf{M}) + \lambda \mathsf{B}$, B étant un entier de $c(\mathsf{M}, \zeta)$. On en tire facilement (comme paragraphe 130)

(90) $$\nu \equiv N_k(\mathsf{A}) \equiv N_k(f(\mathsf{M})), \quad (\mathfrak{l}^l).$$

D'autre part, à cause des congruences

$$a^l \equiv a, \quad a_1^l \equiv a_1, \quad \ldots, \quad a_{l-1}^l \equiv a_{l-1}, \quad (\text{mod } l),$$

on a identiquement en x une égalité

(91) $$f(x) f(\zeta x) \ldots f(\zeta^{l-1} x) = f(x^l) + l F(x^l),$$

où $F(x^l)$ est un polynôme en x^l à coefficients entiers.

On en tire pour $x = 1$, à cause de (89), la congruence

$$f(1) \equiv f(1) + l F(1), \quad (\text{mod } l^2), \qquad \text{c.-à-d.} \qquad F(1) \equiv 0, \quad (\text{mod } l).$$

En faisant $x = \mathsf{M}$ dans (91), on obtient

$$N_k(f(\mathsf{M})) = f(\mu) + l F(\mu),$$

et, par suite, comme on a $F(\mu) \equiv F(1) \equiv 0$, mod $\mathfrak{l}$,

$$N_k(f(\mathsf{M})) \equiv f(\mu), \quad (\text{mod } \mathfrak{l}^l),$$

c'est-à-dire, à cause de (90),

$$\nu \equiv f(\mu), \quad (\text{mod } \mathfrak{l}^l).$$

Ceci joint à (89) démontre complètement le lemme 25.

Lemme 26. — μ et ν étant deux entiers de $c(\zeta)$ tels que l'on ait $\nu \equiv 1$, mod $\mathfrak{l}$, et $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, et ν étant de plus résidu de norme, mod $\mathfrak{l}$, du corps $c(\mathsf{M}, \zeta)$ défini par $\mathsf{M} = \sqrt[l]{\mu}$, on a toujours

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = 1.$$

[Kummer[20].]

Démonstration. — La formule connue de Lagrange pour l'inversion d'une série de puissances donne immédiatement l'identité suivante :

$$(92)\qquad \left[\frac{d^{l-1}\mathrm{F}(v)}{d\mathrm{V}^{l-1}}\right]_{\mathrm{V}=0} = \left[\frac{d^{l-2}\dfrac{d\mathrm{F}(v)}{dv}(\varphi(v))^{l-1}}{dv^{l-2}}\right]_{v=0},$$

dans laquelle $\mathrm{F}(v)$ est une série quelconque de puissances de v, $\varphi(v)$ une série de puissances de v dont le terme constant est $\neq 0$, et V une variable liée à v par l'équation $\mathrm{V}\varphi(v) - v = 0$.

Soient alors $\nu(x)$ et $\mu(x)$ les polynômes adjoints aux nombres ν et μ. Comme ν doit être résidu de normes, mod $\mathfrak{l}$, du corps $c(\mathbf{M}, \zeta)$, il existe (lemme 25) un polynôme $f(x)$ de degré $l-1$ à coefficients entiers, tel que l'on ait

$$(93)\qquad n(f(\zeta)) \equiv 1, \qquad (\mathrm{mod}\ l^2).$$

$$(94)\qquad \nu \equiv f(\mu), \quad (\mathrm{mod}\ \mathfrak{l}^l),$$

et $f(1) > 0$.

Posons alors

$$\mathrm{F}(v) = \log f(\mu(e^v)),$$
$$\mathrm{V} = \log \mu(e^v),$$
$$\varphi(v) = \frac{v}{\log \mu(e^v)}.$$

Ces fonctions ne seront envisagées que pour $v = 0$, et les logarithmes seront déterminés de manière à être réels pour $v = 0$.

Si nous remplaçons ω, $\varpi(x)$ et v dans la deuxième formule $(81)'$, paragraphe 131, par $f(\zeta)$, $f(x)$, V respectivement, on en tire

$$\left[\frac{d^{l-1}\log f(e^{\mathrm{V}})}{d\mathrm{V}^{l-1}}\right]_{\mathrm{V}=0} \equiv l^{(l-1)}(f(\zeta)) + \frac{1 - f(1)}{l}, \quad (\mathrm{mod}\ l).$$

Le lemme 24 donne, vu (93), la congruence

$$l^{(l-1)}(f(\zeta)) \equiv 0, \quad (\mathrm{mod}\ l),$$

et l'on a, par suite,

$$(95)\qquad \left[\frac{d^{l-1}\mathrm{F}(v)}{d\mathrm{V}^{l-1}}\right]_{\mathrm{V}=0} - \left[\frac{d^{l-1}\log f(e^{\mathrm{V}})}{d\mathrm{V}^{l-1}}\right]_{\mathrm{V}=0} \equiv \frac{1 - f(1)}{l}, \quad (\mathrm{mod}\ l),$$

D'autre part, on a, vu (94), la congruence[1]

$$f(\mu(e^v)) \equiv \nu(e^v) + \frac{f(1) - 1}{l}v^{l-1}, \quad (\mathrm{mod}\ l),$$

[1] N. T. — On l'obtient en partant de la deuxième formule $(81)''$, paragraphe 131, en remarquant que, à cause de $\mu \equiv 1 + \lambda$, $(\mathfrak{l}^2)$, on a : $\mu(1) \equiv 1$.

qu'il faut entendre en ce que dans le développement par rapport aux puissances de v les coefficients de $1, v, \ldots, v^{l-1}$ sont congrus, mod l, de part et d'autre, et on en déduit le développement

$$(96)\quad \left\{\begin{aligned} \frac{dF(v)}{dv} \equiv\ & l^{(1)}(\nu) + l^{(2)}(\nu)\frac{v}{1!} + l^{(3)}(\nu)\frac{v^2}{2!} + \ldots \\ & \ldots + \left(l^{(l-1)}(\nu) + \frac{1-\nu^{l-1}}{l}\right)\frac{v^{l-2}}{(l-2)!}, \quad (\mathrm{mod}\ l), \end{aligned}\right.$$

congruence qu'il faut entendre comme exprimant la congruence des coefficients de $1, v, v^2, \ldots, v^{l-2}$.

Considérons enfin la fonction $\varphi(v)$. Comme on a $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, $\varphi(v)$ est une série de puissances dont le terme constant est $\equiv -1$, mod l. Puis on trouve facilement

$$(\varphi(v))^l \equiv \varphi(v^l) \equiv \varphi(0) \equiv -1, \quad (\mathrm{mod}\ l),$$

en ce sens que les coefficients de $1, v, \ldots, v^{l-2}$ sont congrus, mod l, de part et d'autre; puis toujours dans le même sens

$$-(\varphi(v))^{l-1} \equiv \frac{\log \mu(e^v)}{v}, \quad (\mathrm{mod}\ l),$$

et enfin, toujours dans ce même sens, le développement

$$(97)\quad \left\{\begin{aligned} -(\varphi(v))^{l-1} \equiv\ & l^{(1)}(\mu) + l^{(2)}(\mu)\frac{v}{2!} + l^{(3)}(\mu)\frac{v^2}{3!} + \ldots \\ & \ldots + l^{(l-1)}(\mu)\frac{v^{l-2}}{(l-1)!}, \quad (\mathrm{mod}\ l). \end{aligned}\right.$$

La réunion de la congruence (95) et des deux développements (96), (97) avec (92) donne, comme $l^{(l)}(\mu) \equiv -1$ et que $(l-g)!(g-1)! \equiv (-1)^g$, mod l, pour $g = 1, 2, \ldots, l-1$, la congruence suivante :

$$l^{(l-1)}(\nu)\,l^{(1)}(\mu) - l^{(l-2)}(\nu)\,l^{(2)}(\mu) + \ldots - l^{(1)}(\nu)\,l^{(l-1)}(\mu) \equiv 0, \quad (\mathrm{mod}\ l),$$

c'est-à-dire d'après la définition (82) du symbole $\left(\frac{\nu,\mu}{\mathfrak{l}}\right)$ (§ 131),

$$\left(\frac{\nu,\mu}{\mathfrak{l}}\right) = 1,$$

ce qui démontre le lemme 26.

§ 133. — Distinction des résidus et non résidus de normes avec le symbole $\left(\frac{\nu,\mu}{\mathfrak{w}}\right)$.

Théorème 151. — ν, μ étant deux entiers quelconques de $k(\zeta)$, mais $\sqrt[l]{\mu}$ n'étant pas dans $k(\zeta)$, et $\mathfrak{w}$ étant un idéal premier quelconque du corps circulaire $k(\zeta)$, ν est résidu ou non résidu de normes, mod $\mathfrak{w}$, du corps kummerien $k(M, \zeta)$ défini par $M = \sqrt[l]{\mu}$, suivant que l'on a

$$\left(\frac{\nu,\mu}{\mathfrak{w}}\right) = 1 \quad \text{ou} \quad = -1.$$

Démonstration. — Soit d'abord $\mathfrak{w} \neq \mathfrak{l}$ et ne divisant pas le discriminant relatif du corps $c(\mathsf{M}, \zeta)$. Si μ^* est un entier de $c(\zeta)$, tel que $\frac{\mu^*}{\mu}$ soit la $l^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$, on a toujours $\left(\frac{\nu, \mu^*}{\mathfrak{w}}\right) = \left(\frac{\nu, \mu}{\mathfrak{w}}\right)$. On peut donc, vu le théorème 148, admettre ici que μ n'est pas divisible par $\mathfrak{w}$. Distinguons deux cas, suivant que $\mathfrak{w}$ est égal dans $c(\mathsf{M}, \zeta)$ à un produit de l idéaux premiers $\mathfrak{W}_1, \ldots, \mathfrak{W}_l$ ou que $\mathfrak{w}$ est lui-même idéal premier dans $c(\mathsf{M}, \zeta)$. D'après le théorème 149 on a, dans le premier cas $\left(\frac{\mu}{\mathfrak{w}}\right) = 1$, dans le second $\left(\frac{\mu}{\mathfrak{w}}\right) \neq 1$ et $\neq 0$.

Dans le premier cas déterminons un entier A de $c(\mathsf{M}, \zeta)$ divisible par $\mathfrak{W}_1$ mais non par $\mathfrak{W}_1^2$ ni par aucun des idéaux $\mathfrak{W}_2, \ldots, \mathfrak{W}_l$; alors la norme relative $\alpha = \mathrm{N}_c(\mathsf{A})$ contient $\mathfrak{w}$ exactement au premier degré. Si alors $\mathfrak{w}^b$ est la puissance de $\mathfrak{w}$ contenue dans ν, $x = \frac{\nu}{\alpha^b}$ peut se mettre sous forme d'une fraction dont les deux termes sont premiers à $\mathfrak{w}$ et sont, par suite (théorème 150), résidus de normes du corps $c(\mathsf{M}, \zeta)$, mod $\mathfrak{w}$. Il en est donc de même de ν. Comme, d'après la définition du paragraphe 131,

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \left(\frac{\mu^b}{\mathfrak{w}}\right)^{-1} = 1,$$

le théorème 151 est exact dans ce premier cas.

Dans le second cas, la norme relative d'un entier A de $c(\mathsf{M}, \zeta)$ est toujours divisible exactement par une puissance de $\mathfrak{w}$ dont l'exposant est un multiple de l. Soit encore $\mathfrak{w}^b$ la puissance de $\mathfrak{w}$ contenue dans ν; si b n'est pas multiple de l, ν ne peut donc être résidu de normes, mod $\mathfrak{w}$; dans ce cas, on a d'ailleurs

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \left(\frac{\mu^b}{\mathfrak{w}}\right)^{-1} \neq 1.$$

Si au contraire b est un multiple de l, et que α désigne un entier de $c(\zeta)$ divisible par $\mathfrak{w}$, non par $\mathfrak{w}^2$, nous posons $x = \frac{\nu}{\alpha^b}$ et nous voyons que ν est résidu de normes, mod $\mathfrak{w}$, comme dans le premier cas; d'autre part, on a maintenant

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \left(\frac{\mu^b}{\mathfrak{w}}\right)^{-1} = 1.$$

Le théorème 151 est ainsi démontré dans ce second cas.

Supposons maintenant que le discriminant relatif du corps $c(\mathsf{M}, \zeta)$ soit divisible par l'idéal premier $\mathfrak{w}$; $\mathfrak{w}$ doit être $\neq \mathfrak{l}$. Supposons que ν soit divisible par $\mathfrak{w}^b$ et μ par $\mathfrak{w}^a$; alors a n'est en tout cas jamais multiple de l. Le nombre $x = \frac{\nu^a}{\mu^b}$ peut se mettre sous forme d'une fraction $\frac{\rho}{\sigma}$, dont les deux termes sont premiers à $\mathfrak{w}$. Le

nombre $\rho\sigma^{l-1}$ est un entier non divisible par $\mathfrak{w}$; d'après la démonstration du théorème 150, pour qu'un tel nombre soit résidu de normes, mod $\mathfrak{w}$, il faut et il suffit qu'il soit résidu de $l^{ième}$ puissance, mod $\mathfrak{w}$, c'est-à-dire ici, que $\left\{\frac{\rho\sigma^{l-1}}{\mathfrak{w}}\right\} = 1$ et par suite que $\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\} = 1$; le théorème 151 est encore exact dans ce cas.

Soit enfin $\mathfrak{w} = \mathfrak{l}$. Nous envisagerons seulement le cas où l'on a $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$ (le seul dont nous aurons besoin dans la suite; les autres se traiteraient d'une manière analogue). Pour la démonstration, nous ferons encore la restriction (non essentielle) $\nu \equiv 1$, mod $\mathfrak{l}$. Comme on a $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, on peut, d'après le théorème 150, former exactement l^{l-1} résidus de normes ν^* du corps $c(\mathsf{M}, \zeta)$, mod $\mathfrak{l}$, résidus congrus à 1, mod $\mathfrak{l}$, et incongrus entre eux mod $\mathfrak{l}^{l+1}$. D'autre part, tout résidu de normes ν^* de $c(\mathsf{M}, \zeta)$, mod $\mathfrak{l}$, pour lequel on a $\nu^* \equiv 1$, mod $\mathfrak{l}$, remplit (lemme 26) la condition $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = 1$.

A cause de

$$\left.\begin{aligned} &l^{(1)}(\mu) \equiv -1,\\ &l^{(1)}(1-l) \equiv 0,\quad l^{(2)}(1-l) \equiv 0,\quad \ldots,\quad l^{(l-2)}(1-l) \equiv 0,\\ &l^{(l-1)}(1-l) - \frac{1-n(1-l)}{l} \equiv -1, \end{aligned}\right\} \pmod{l},$$

on obtient, vu (82) :

$$\left\{\frac{1-l,\ \mu}{\mathfrak{l}}\right\} = \zeta^{-1}. \tag{98}$$

Soit maintenant α un entier quelconque de $c(\zeta)$ congru à 1, mod $\mathfrak{l}$, et posons

$$\left\{\frac{\alpha,\ \mu}{\mathfrak{l}}\right\} = \zeta^{a},$$

où a est un nombre de la suite 0, 1, 2, ..., $l-1$; alors on a évidemment

$$\left\{\frac{\alpha(1-l)^{a},\ \mu}{\mathfrak{l}}\right\} = 1 ;$$

au contraire, on a toujours

$$\left\{\frac{\alpha(1-l)^{x},\ \mu}{\mathfrak{l}}\right\} \neq 1$$

lorsque x est un nombre de la suite 0, 1, 2, ..., $l-1$, $\neq a$. Si nous choisissons ensuite un entier α' de $c(\zeta)$, encore congru à 1, mod $\mathfrak{l}$, mais non congru, mod $\mathfrak{l}$, à aucun des l nombres α, $\alpha(1-l)$, $\alpha(1-l)^2$, ..., $\alpha(1-l)^{l-1}$, les l nombres α', $\alpha'(1-l)$, $\alpha'(1-l)^2$, ..., $\alpha'(1-l)^{l-1}$ sont aussi tous incongrus entre eux, mod $\mathfrak{l}^{l+1}$, et de plus non congrus à aucun des l premiers nombres; parmi ces l derniers nombres, il y en a évidemment, à cause de (98), un et un seul — soit, par exemple, $\alpha'(1-l)^{a'}$ — tel

que $\left\{\frac{\alpha'(1-l)^{m},\ \mu}{\mathfrak{l}}\right\}=1$. En continuant ainsi, nous voyons que le nombre des nombres ν incongrus, mod $\mathfrak{l}^{l+1}$, congrus à 1, mod $\mathfrak{l}$, et vérifiant la condition $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}=1$, est précisément l^{l-1}, et comme ce nombre coïncide avec le nombre trouvé antérieurement pour les résidus des normes ν^{*}, on voit qu'inversement tout nombre ν possédant ces deux propriétés est résidu de normes du corps $c(\mathsf{M},\ \zeta)$, mod $\mathfrak{l}$.

Le théorème 151 est ainsi démontré complètement; à part que pour le cas de $\mathfrak{w}=\mathfrak{l}$ on s'est borné aux nombres ν, μ, $\nu\equiv 1$, mod $\mathfrak{l}$, et $\mu\equiv 1+\lambda$, mod $\mathfrak{l}^2$. La restriction relative à ν est évidemment facile à lever.

Du théorème 151 résulte, à l'aide des premières formules (80) et (83), la formule

$$\left\{\frac{\nu\nu^{*},\ \mu}{\mathfrak{w}}\right\}=\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\},$$

où $\mathfrak{w}$ est un idéal premier quelconque de $c(\zeta)$ et ν^{*} un résidu de normes du corps $c(\mathsf{M},\ \zeta)$, mod $\mathfrak{w}$.

Pour définir maintenant le symbole $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ dans le cas où l'un des deux nombres ν, μ ou tous les deux sont divisibles par $\mathfrak{l}$, il suffit de convenir qu'on a toujours les formules

$$\left\{\frac{\nu\nu^{0},\ \mu}{\mathfrak{l}}\right\}=\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\},\qquad \left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\ \nu}{\mathfrak{l}}\right\}=1,$$

où ν^{0} est un résidu de normes quelconque du corps $c(\sqrt[l]{\mu},\ \zeta)$, mod $\mathfrak{l}$. On en déduit, en particulier (1),

$$\left\{\frac{1+a\lambda^{l},\ \lambda}{\mathfrak{l}}\right\}=\left\{\frac{1+a\lambda^{l}}{\mathfrak{l}}\right\}=\zeta^{a}.$$

Nous pourrions uniquement baser la définition du *symbole* $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ sur les formules

$$\left\{\frac{\alpha,\ \zeta}{\mathfrak{l}}\right\}=\zeta^{\frac{n(\alpha)-1}{l}},\qquad \left\{\frac{\nu_1\nu_2,\ \mu}{\mathfrak{l}}\right\}=\left\{\frac{\nu_1,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2,\ \mu}{\mathfrak{l}}\right\},$$

$$\left\{\frac{\nu^{*},\ \mu}{\mathfrak{l}}\right\}=1,\qquad \left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\ \nu}{\mathfrak{l}}\right\}=1,$$

(1) N. T.

$$\left\{\frac{1+a\lambda^{l},\ \lambda}{\mathfrak{l}}\right\}=\left\{\frac{\lambda,\ 1+a\lambda^{l}}{\mathfrak{l}}\right\}^{-1}.$$

ν est ici divisible par $\mathfrak{l}^1$ et μ par $\mathfrak{l}^0$; donc .

$$\alpha=\frac{\nu^{0}}{\mu^{1}}=\frac{1}{1+a\lambda^{l}},\qquad \rho=1,\qquad \sigma=1+a\lambda^{l},$$

$$\left\{\frac{\lambda,\ 1+a\lambda^{l}}{\mathfrak{l}}\right\}=\left\{\frac{1}{\mathfrak{l}}\right\}\left\{\frac{1+a\lambda^{l}}{\mathfrak{l}}\right\}^{-1},\qquad \left\{\frac{1+a\lambda^{l},\ \lambda}{\mathfrak{l}}\right\}=\left\{\frac{1+a\lambda^{l}}{\mathfrak{l}}\right\}=\zeta^{a}.$$

où α est un entier de $c(\zeta)$ premier à $\mathfrak{l}$, ν un résidu de normes de $c(\sqrt[l]{\mu}, \zeta)$, mod $\mathfrak{l}$, et ν, ν_1, ν_2 des entiers quelconques de $c(\zeta)$ (voir § 166). J'ai pourtant choisi pour le moment la définition (82), qui se rattache immédiatement aux développements de Kummer.

Remarquons enfin que nous avons maintenant atteint le but fixé au début du paragraphe 131 ; si, en effet, $\mathfrak{w}^e$ est une puissance quelconque de l'idéal premier $\mathfrak{w}$ (avec $e > l$ dans le cas où $\mathfrak{w} = \mathfrak{l}$), on peut évidemment diviser un système complet de nombres de $c(\zeta)$ premiers à $\mathfrak{w}$ et incongrus, mod $\mathfrak{w}^e$, en ayant égard aux valeurs du symbole $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ en l sections contenant toutes autant de nombres, l'une d'elles contenant tous les résidus de normes mod $\mathfrak{w}$ du corps $c(\mathsf{M}, \zeta)$ se trouvant dans le système.

CHAPITRE XXX.

Existence d'une infinité d'idéaux premiers ayant des caractères de puissances donnés dans un corps kummerien.

§ 134. — Valeur limite d'un produit infini.

Après avoir, au paragraphe 128, obtenu tous les idéaux premiers d'un corps kummerien, nous sommes en mesure de faire pour ce corps les mêmes recherches qu'aux paragraphes 79 et 80 pour le corps quadratique. Nous commencerons par l'importante proposition suivante :

Lemme 27. — l désignant un nombre premier impair et α un entier quelconque du corps circulaire défini par $\zeta = e^{\frac{2i\pi}{l}}$, non égal à la $l^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$, le produit

$$\prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left\{\frac{\alpha}{\mathfrak{p}}\right\}^m n(\mathfrak{p})^{-s}}$$

a toujours une limite finie et différente de 0 pour $s = 1$; le produit $\prod_{(\mathfrak{p})}$ étant étendu à tous les idéaux premiers de $c(\zeta)$ et le produit $\prod_{(m)}$ à tous les exposants $m = 1, 2, \ldots, l - 1$. [Kummer[20].]

Démonstration. — En envisageant le corps kummerien $C = c(\sqrt[l]{\alpha}, \zeta)$ et désignant ici la fonction $\zeta(s)$ du théorème 56 par $\zeta_1(s)$, on a, d'après le paragraphe 27,

$$\zeta_1(s) = \prod_{(\mathfrak{P})} \frac{1}{1 - N(\mathfrak{P})^{-s}},$$

le produit étant étendu à tous les idéaux premiers $\mathfrak{P}$ de C et $N(\mathfrak{P})$ étant la norme de $\mathfrak{P}$ prise dans C. Si l'on ordonne ce produit par rapport aux idéaux premiers $\mathfrak{p}$ du corps $c(\zeta)$, dont proviennent les idéaux premiers $\mathfrak{P}$, à chaque idéal $\mathfrak{p}$ correspond dans le produit (théorème 149) le terme

$$\frac{1}{(1 - n(\mathfrak{p})^{-s})^l}, \quad \text{ou} \quad \frac{1}{1 - n(\mathfrak{p})^{-s}}, \quad \text{ou} \quad \frac{1}{1 - n(\mathfrak{p})^{-ls}},$$

suivant que l'on a $\left(\frac{\alpha}{\mathfrak{p}}\right) = 1$ ou $= 0$, ou $\neq 1$ et $\neq 0$.

Ecrivons ces trois expressions sous une forme commune :

$$\frac{1}{1 - n(\mathfrak{p})^{-s}} \prod_{(m)} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right)^m n(\mathfrak{p})^{-s}} \qquad (\text{pour } m = 1, 2, \ldots, l-1);$$

nous obtenons ainsi

$$(99) \qquad \zeta_1(s) = \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}} \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left(\frac{\alpha}{\mathfrak{p}}\right)^m n(\mathfrak{p})^{-s}},$$

$\prod_{(m)}$ représentant le produit étendu à $m = 1, 2, \ldots, l - 1$ et les deux produits $\prod_{(\mathfrak{p})}$ s'étendant à tous les idéaux premiers $\mathfrak{p}$ de $c(\zeta)$. Or, chacune des expressions

$$\operatorname*{Lim}_{s=1} (s - 1) \prod_{(\mathfrak{p})} \frac{1}{1 - n(\mathfrak{p})^{-s}}, \qquad \operatorname*{Lim}_{s=1} (s - 1) \zeta_1(s)$$

est finie et $\neq 0$, comme on le voit en appliquant le théorème 56 au corps circulaire $c(\zeta)$, puis au corps kummerien $C = c(\sqrt[l]{\alpha}, \zeta)$. En multipliant par $s - 1$ l'équation (99) et passant à la limite pour $s = 1$, on voit que l'expression donnée dans le lemme 27 a une limite finie et $\neq 0$.

§ 135. — Idéaux premiers de $c(\zeta)$ ayant des caractères de puissances donnés.

Théorème 152. — Soient $\alpha_1, \ldots, \alpha_t$, t entiers quelconques du corps circulaire $c(\zeta)$, tels que le produit

$$\alpha_1^{m_1} \alpha_2^{m_2} \ldots \alpha_t^{m_t}$$

ne soit jamais la puissance $l^{\text{ième}}$ d'un nombre de $c(\zeta)$ lorsque $m_1, m_2, \ldots, m_t$ prennent les valeurs 0, 1, ..., $l - 1$, la combinaison $m_1 = m_2 = \ldots = m_t = 0$ exclue; soient

de plus $\gamma_1, \gamma_2, \ldots, \gamma_t$ des racines $l^{\text{ièmes}}$ de l'unité données arbitrairement. Il y a toujours dans le corps circulaire $c(\zeta)$ une infinité d'idéaux premiers $\mathfrak{p}$, tels que l'on ait pour un certain exposant m premier à l

$$\left(\frac{\alpha_1}{\mathfrak{p}}\right)^m = \gamma_1, \quad \left(\frac{\alpha_2}{\mathfrak{p}}\right)^m = \gamma_2, \quad \ldots, \quad \left(\frac{\alpha_t}{\mathfrak{p}}\right)^m = \gamma_t.$$

[Kummer[20].]

Démonstration. — On a, tant que s est > 1,

$$(100)\quad \begin{cases} \log \sum\limits_{(\mathfrak{j})} \dfrac{1}{n(\mathfrak{j})^s} = \sum\limits_{(\mathfrak{p})} \log \dfrac{1}{1 - n(\mathfrak{p})^{-s}} = \sum\limits_{(\mathfrak{p})} \dfrac{1}{n(\mathfrak{p})^s} + S, \\ S = \frac{1}{2} \sum\limits_{(\mathfrak{p})} \dfrac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3} \sum\limits_{(\mathfrak{p})} \dfrac{1}{n(\mathfrak{p})^{3s}} + \ldots, \end{cases}$$

où $\sum\limits_{(\mathfrak{j})}$ et $\sum\limits_{(\mathfrak{p})}$ sont étendus respectivement à tous les idéaux et à tous les idéaux premiers de $c(\zeta)$. Comme l'expression S reste finie pour $s = 1$ (voir § 50), il résulte de (100) que, le premier membre devenant infini pour $s = 1$, la somme $\sum\limits_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s}$ croît également au delà de toute limite lorsque s tend vers 1. Ensuite, α étant un nombre entier quelconque de $c(\zeta)$, on a de même pour $s > 1$

$$(101)\quad \begin{cases} \log \prod\limits_{(\mathfrak{p})} \dfrac{1}{1 - \left(\dfrac{\alpha}{\mathfrak{p}}\right) n(\mathfrak{p})^{-s}} = \sum\limits_{(\mathfrak{p})} \left(\dfrac{\alpha}{\mathfrak{p}}\right) \dfrac{1}{n(\mathfrak{p})^s} + S(\alpha), \\ S(\alpha) = \frac{1}{2} \sum\limits_{(\mathfrak{p})} \left(\dfrac{\alpha}{\mathfrak{p}}\right)^2 \dfrac{1}{n(\mathfrak{p})^{2s}} + \frac{1}{3} \sum\limits_{(\mathfrak{p})} \left(\dfrac{\alpha}{\mathfrak{p}}\right)^3 \dfrac{1}{n(\mathfrak{p})^{3s}} + \ldots, \end{cases}$$

et $S(\alpha)$ reste ici encore finie pour $s = 1$. Soit maintenant m un des nombres 1, 2, ..., $l - 1$. Posons dans (101) $\alpha = \alpha_u^m = \alpha_1^{mu_1} \alpha_2^{mu_2} \ldots \alpha_t^{mu_t}$ et multiplions encore l'égalité obtenue par le facteur $\gamma_1^{-u_1} \gamma_2^{-u_2} \ldots \gamma_t^{-u_t}$; donnons ensuite à chacun des t exposants $u_1, u_2, \ldots, u_t$ les l valeurs 0, 1, 2, ..., $l - 1$ (à l'exclusion de la combinaison $u_1 = u_2 = \ldots = u_t = 0$). En additionnant les $l^t - 1$ égalités ainsi obtenues à (100), on obtient la relation

$$(102)\quad \begin{cases} \sum\limits_{(\mathfrak{p})} \dfrac{1}{n(\mathfrak{p})^s} + S + \sum\limits_{(u_1, \ldots, u_t)} \gamma_1^{-u_1} \ldots \gamma_t^{-u_t} \log \prod\limits_{(\mathfrak{p})} \dfrac{1}{1 - \left(\dfrac{\alpha_1^{u_1} \ldots \alpha_t^{u_t}}{\mathfrak{p}}\right)^m n(\mathfrak{p})^{-s}} \\ = \sum\limits_{(\mathfrak{p})} [1][2] \ldots [t] \dfrac{1}{n(\mathfrak{p})^s} + S + \sum\limits_{(u_1, \ldots, u_t)} \gamma_1^{-u_1} \ldots \gamma_t^{-u_t} S(\alpha^m), \end{cases}$$

où l'on a posé pour un instant

$$[1] = 1 + \left(\gamma_1^{-1}\left(\frac{\alpha_1}{\mathfrak{p}}\right)^m\right) + \left(\gamma_1^{-1}\left(\frac{\alpha_1}{\mathfrak{p}}\right)^m\right)^2 + \ldots + \left(\gamma_1^{-1}\left(\frac{\alpha_1}{\mathfrak{p}}\right)^m\right)^{l-1},$$

$$[2] = 1 + \left(\gamma_2^{-1}\left(\frac{\alpha_2}{\mathfrak{p}}\right)^m\right) + \left(\gamma_2^{-1}\left(\frac{\alpha_2}{\mathfrak{p}}\right)^m\right)^2 + \ldots + \left(\gamma_2^{-1}\left(\frac{\alpha_2}{\mathfrak{p}}\right)^m\right)^{l-1},$$

. . . .

$$[t] = 1 + \left(\gamma_t^{-1}\left(\frac{\alpha_t}{\mathfrak{p}}\right)^m\right) + \left(\gamma_t^{-1}\left(\frac{\alpha_t}{\mathfrak{p}}\right)^m\right)^2 + \ldots + \left(\gamma_t^{-1}\left(\frac{\alpha_t}{\mathfrak{p}}\right)^m\right)^{l-1}.$$

Faisons abstraction, dans la première somme du second membre de 102, des termes en nombre limité (dont G_m désignera l'ensemble), correspondant aux facteurs idéaux premiers de $\alpha_1, \ldots, \alpha_t, \lambda$. Le reste infini de cette somme est alors évidemment $l^t \sum_{\mathfrak{q}} \frac{1}{n(\mathfrak{q})^s}$, où $\mathfrak{q}$ parcourt seulement tous les idéaux premiers de $c(\zeta)$, remplissant les t conditions

$$(103) \qquad \left(\frac{\alpha_1}{\mathfrak{p}}\right)^m = \gamma_1, \quad \ldots, \quad \left(\frac{\alpha_t}{\mathfrak{p}}\right)^m = \gamma_t.$$

Écrivons alors les égalités (102) les unes après les autres pour $m = 1, 2, \ldots, l-1$ et ajoutons ; nous obtenons

$$(104) \quad \left\{ \begin{aligned} &(l-1)\sum_{(\mathfrak{p})} \frac{1}{n(\mathfrak{p})^s} + (l-1)S \\ &+ \sum_{(u_1, \ldots, u_t)} \gamma_1^{-u_1} \ldots \gamma_t^{-u_t} \log \prod_{(\mathfrak{p})} \prod_{(m)} \frac{1}{1 - \left(\frac{\alpha_1^{u_1} \ldots \alpha_t^{u_t}}{\mathfrak{p}}\right)^m n(\mathfrak{p})^{-s}} \\ &= l^t \sum_{(\mathfrak{r})} \frac{1}{n(\mathfrak{r})^s} + \sum_{(m)} G_m + (l-1)S + \sum_{(u_1, \ldots, u_t)} \gamma_1^{-u_1} \ldots \gamma_t^{-u_t} \sum S(\alpha_0^m) ; \end{aligned} \right.$$

$\mathfrak{r}$ parcourt tous les idéaux premiers $\mathfrak{p}$ de $c(\zeta)$ satisfaisant à l'un quelconque des $l-1$ systèmes de conditions (103) obtenus en faisant $m = 1, 2, \ldots, l-1$; pour $\gamma_1 = 1, \ldots, \gamma_t = 1$, ces $l-1$ systèmes sont identiques et les idéaux premiers correspondants doivent être pris $l-1$ fois. En passant alors à la limite pour $s = 1$, la première somme Σ du premier membre de 104 augmente indéfiniment, tandis que la deuxième somme Σ du premier membre reste finie d'après le lemme (27). S et $S(\alpha_0^m)$ restant aussi finies, l'expression $\sum \frac{1}{n(\mathfrak{r})^s}$ croît donc indéfiniment lorsque s tend vers 1, et, par suite, il y a une infinité d'idéaux $\mathfrak{r}$; or, ils satisfont au théorème 152.

CHAPITRE XXXI.

Corps circulaires réguliers.

§ 136. — Définition des corps circulaires réguliers, des nombres premiers réguliers et des corps kummeriens réguliers.

Soit l premier impair, $\zeta = e^{\frac{2i\pi}{l}}$; le corps circulaire $c(\zeta)$ et le nombre premier l seront *réguliers*, lorsque le nombre h des classes d'idéaux du corps $c(\zeta)$ ne sera pas divisible par l. Les chapitres suivants ne traiteront que des corps circulaires réguliers et des corps kummeriens qui en résultent, corps que j'appellerai *corps kummeriens réguliers*; on peut démontrer de suite pour ces derniers la proposition simple ci-après.

Théorème 153. — Soit $c(\zeta)$ un corps circulaire régulier et C un corps kummerien déduit de $c(\zeta)$: tout idéal $\mathfrak{j}$ de $c(\zeta)$ qui est idéal principal de C est aussi principal dans c.

Démonstration. — Posons $\mathfrak{j} = (\mathbf{A})$. $\mathbf{A}$ étant un entier de C, on a en formant la norme relative $\mathfrak{j}^l = (\mathrm{N}_c(\mathbf{A}))$, c'est-à-dire qu'on a dans $c(\zeta)$ l'équivalence $\mathfrak{j}^l \sim 1$. D'un autre côté, on a aussi $\mathfrak{j}^h \sim 1$, h étant le nombre de classes de $c(\zeta)$. En déterminant deux entiers positifs a et b, tels que $al - bh = 1$, on a donc $\mathfrak{j}^{al-bh} \sim 1$, c'est-à-dire que $\mathfrak{j}$ est idéal principal dans $c(\zeta)$.

La question se pose de trouver un critérium pour reconnaître simplement si un nombre premier l est régulier. Les deux lemmes ci-après vont nous conduire à ce critérium.

§ 137. — Lemme sur la divisibilité par l du premier facteur du nombre de classes de $c\left(e^{\frac{2i\pi}{l}}\right)$.

Lemme 28. — l étant premier impair, la condition nécessaire et suffisante pour que le premier facteur du nombre de classes du corps $c\left(\zeta = e^{\frac{2i\pi}{l}}\right)$ soit divisible par l est que l divise le numérateur de l'un des $l^* = \frac{l-3}{2}$ premiers nombres de Bernoulli. [Kummer[8], Kronecker[5].]

Démonstration. — On a mis, au théorème 142, le nombre de classes h du corps $c(\zeta)$ sous forme d'un produit de deux facteurs; considérons l'expression donnée au premier. Posons pour abréger $Z = e^{\frac{2i\pi}{l-1}}$. Supposons de plus r racine primitive mod l, choisie de façon que $r^{\frac{l-1}{2}} + 1$ ne soit divisible que par la première puissance de l[1]. Soit enfin, comme aux paragraphes 108 et 109, r_i le plus petit reste positif de r^i mod l et $q_i = \dfrac{r r_i - r_{i+1}}{l}$.

Le premier facteur du nombre de classes h est mis dans le théorème 142 sous la forme d'une fraction dont le dénominateur est $(2l)^{l^*}$, et dont le numérateur est

$$(105) \qquad f(Z) f(Z^3) f(Z^5) \ldots f(Z^{l-2}),$$

$f(x)$ désignant pour abréger le polynôme à coefficients entiers

$$f(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{l-2} x^{l-2}.$$

En posant ensuite

$$g(x) = q_0 + q_1 x + q_2 x^2 + \ldots + q_{l-2} x^{l-2},$$

on trouve aisément

$$(rZ - 1) f(Z) = lZ \cdot g(Z),$$

et comme, vu le choix de r, le produit

$$(rZ - 1)(rZ^3 - 1) \ldots (rZ^{l-2} - 1) = (-1)^{\frac{l-1}{2}} (r^{\frac{l-1}{2}} + 1)$$

est exactement divisible par la première puissance de l, il en résulte que le numérateur (105) du premier facteur de h n'est divisible par $l^{\frac{l-1}{2}} = l^{l^*+1}$ que si le nombre

$$g(Z) g(Z^3) \ldots g(Z^{l-2})$$

est divisible par l. Maintenant $\mathfrak{L} = (l, Z - r)$ est un idéal premier diviseur de l dans le corps $c(Z)$, et comme on a évidemment $Z \equiv r$, mod $\mathfrak{L}$, on a

$$g(Z) g(Z^3) \ldots (gZ^{l-2}) \equiv g(r) \ldots g(r^{l-2}), \quad (\text{mod } \mathfrak{L});$$

par suite, le premier facteur du nombre de classes h n'est divisible par l que si l'une au moins des $\dfrac{l-1}{2}$ congruences

$$g(r^{2i-1}) = q_0 + q_1 r^{2i-1} + q_2 r^{2(2i-1)} + \ldots + q_{l-2} r^{(l-2)(2i-1)} \equiv 0, \quad (\text{mod } l),$$
$$\left(i = 1, 2, \ldots, \tfrac{l-1}{2}\right)$$

est vérifiée.

---

(1) N. T. — Si l'on avait $r^{\frac{l-1}{2}} + 1 \equiv 0$, (l^2), il suffirait de prendre une racine $r' \equiv r$, (l) et $\not\equiv r$, (l^2).

Soit alors t un des nombres $1, 2, 3, \ldots, \frac{l-1}{2}$. En élevant à la puissance $2t$ l'identité

$$rr_i = r_{i+1} + (rr_i - r_{i+1}),$$

dans laquelle $rr_i - r_{i+1}$ est divisible par l, on obtient la congruence

$$r^{2t} r_i^{2t} \equiv r_{i+1}^{2t} + 2t(rr_i - r_{i+1}) r_{i+1}^{2t-1}, \quad (\text{mod } l^2),$$

ou

$$2t(rr_i - r_{i+1}) r_{i+1}^{2t-1} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \quad (\text{mod } l^2);$$

et comme on a évidemment

$$(rr_i - r_{i+1}) r_{i+1}^{2t-1} \equiv (rr_i - r_{i+1}) r^{(i+1)(2t-1)}, \quad (\text{mod } l^2),$$

on en tire

$$2t(rr_i - r_{i+1}) r^{(i+1)(2t-1)} \equiv r^{2t} r_i^{2t} - r_{i+1}^{2t}, \quad (\text{mod } l^2).$$

En ajoutant ces congruences pour $i = 0, 1, 2, \ldots, l-2$, on obtient

$$2tl r^{2t-1} \sum_{(i)} q_i r^{i(2t-1)} \equiv r^{2t} \sum_{(i)} r_i^{2t} - \sum_{(i)} r_{i+1}^{2t}, \quad (\text{mod } l^2).$$

Comme d'ailleurs on a

$$\sum_{(i)} r_i^{2t} = \sum_{(i)} r_{i+1}^{2t} = 1^{2t} + 2^{2t} + 3^{2t} + \ldots + (l-1)^{2t},$$

il en résulte que la condition nécessaire et suffisante pour que le nombre $g(r^{2t-1})$ soit divisible par l est que le nombre

(106) $$(r^{2t} - 1)(1^{2t} + 2^{2t} + \ldots + (l-1)^{2t})$$

soit divisible par l^2. Vu l'hypothèse faite pour la racine primitive r, l'expression (106) n'est certainement pas divisible par l^2 pour $t = \frac{l-1}{2}$. Pour $t = 1, 2, \ldots, \frac{l-3}{2}$ on a toujours, d'après la formule sommatoire de Bernoulli [1], la congruence

$$1^{2t} + 2^{2t} + 3^{2t} + \ldots + (l-1)^{2t} \equiv (-1)^{t-1} B_t l, \quad (\text{mod } l^2).$$

---

[1] N. T. — Rappelons qu'on appelle *nombres de Bernoulli* les coefficients $B_1, B_2, \ldots$, du développement

(1) $$\frac{x}{e^x - 1} + \frac{x}{2} = \frac{x}{2} \frac{e^x + 1}{e^x - 1} = 1 + \frac{B_1 x^2}{2!} - \frac{B_2 x^4}{4!} + \ldots + \frac{(-1)^{n-1} B_n x^{2n}}{(2n)!} - \ldots$$

Valeurs des premiers :

$$B_1 = \frac{1}{6}, \quad B_2 = \frac{1}{30}, \quad B_3 = -\frac{1}{42}, \quad B_4 = \frac{1}{30}, \quad B_5 = \frac{5}{66}, \quad B_6 = \frac{691}{2730}, \quad B_7 = \frac{7}{6}, \quad \ldots$$

On appelle *polynômes de Bernoulli* les polynômes $\varphi_p(x)$ s'annulant pour $x = 0$ et vérifiant

où B_t représente le $t^{\text{ième}}$ *nombre de Bernoulli*, et, par suite, la divisibilité par l^e de l'un au moins des nombres (106) pour $t = 1, 2, \ldots \frac{l-3}{2}$ revient à la divisibilité par l d'au moins un des numérateurs des $\frac{l-3}{2}$ premiers nombres de Bernoulli. Le lemme 28 est ainsi démontré.

§ 138. — Lemme sur les unités du corps circulaire $c\left(e^{\frac{2i\pi}{l}}\right)$ dans le cas où l ne divise le numérateur d'aucun des $\frac{l-3}{2}$ premiers nombres de Bernoulli.

Lemme 29. — l étant un nombre premier impair ne divisant le numérateur d'aucun des $\frac{l-3}{2} = l^*$ premiers nombres de Bernoulli, on peut toujours former, au

---

l'équation fonctionnelle

$$(2) \qquad \varphi_p(x) - \varphi_p(x-1) = x^p.$$

On a

$$(3) \qquad \varphi_p(n) = 1^p + 2^p + 3^p + \ldots + (n-1)^p + n^p.$$

On démontre l'expression ci-après de ce polynôme :

$$\varphi_p(x) = \frac{x^{p+1}}{p+1} + \frac{x^p}{2} + B_1 \frac{p}{2!} x^{p-1} - B_2 \frac{p(p-1)(p-2)}{4!} x^{p-3}$$
$$+ B_3 \frac{p(p-1)\ldots(p-4)}{6!} x^{p-5} - \ldots .$$

On trouve en effet, à l'aide du développement (1), en chassant le dénominateur $e^x - 1$, divisant par x les deux membres et égalant les coefficients de x^{2n}, la formule de récurrence

$$\frac{1}{2.(2n)!} = \frac{(-1)^{n-1} B_n}{(2n)!\,1!} + \frac{(-1)^n B_{n-1}}{(2n-2)!\,3!} + \ldots + \frac{B_1}{2!\,(2n-1)!} + \frac{1}{(2n+1)!}.$$

Or, on est conduit à la même formule en égalant les coefficients de x^{p-2n} dans les deux membres de l'équation fonctionnelle (2) : $\varphi_p(x) - \varphi_p(x-1) = x^p$.

Des propriétés ci-dessus résulte l'égalité

$$\varphi_{2p}(n) = 1^{2p} + 2^{2p} + \ldots + (n-1)^{2p} + n^{2p} = \frac{n^{2p+1}}{2p+1} + \frac{n^{2p}}{2} + B_1 \frac{2p}{2!} n^{2p-1}$$
$$- B_2 \frac{2p(2p-1)(2p-2)}{4!} n^{2p-3} + \ldots + (-1)^{p-1} B_p \frac{(2p)!}{(2p)!} n ;$$

d'où la congruence indiquée.

moyen de produits et quotients d'unités du corps circulaire $c(\zeta)$, un système de l^* unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ vérifiant les l^* congruences

(107)
$$\begin{cases} \varepsilon_1 \equiv 1 + a_1\lambda^2, & (\mathfrak{l}^3), \\ \varepsilon_2 \equiv 1 + a_2\lambda^4, & (\mathfrak{l}^5), \\ \varepsilon_3 \equiv 1 + a_3\lambda^6, & (\mathfrak{l}^7), \\ \cdots\cdots\cdots & \\ \varepsilon_{l^*} \equiv 1 + a_{l^*}\lambda^{l-3}, & (\mathfrak{l}^{l-2}), \end{cases}$$

où $a_1, a_2, \ldots, a_{l^*}$ sont des entiers rationnels non divisibles par l, et où on a posé $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$. [Kummer[12].]

Démonstration. — Partons de l'unité circulaire (v. § 98)

(108)
$$\varepsilon = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}},$$

où r est une racine primitive mod l. Posons ensuite $\varepsilon^{l-1} = \eta_1$ et

(109)
$$\varepsilon_t = \eta_1^{(r^2-s)(r^4-s)(r^6-s)\ldots(r^{2t-2}-s)(r^{2t+2}-s)(r^{2t+4}-s)\ldots(r^{l-3}-s)}$$

pour $t = 1, 2, 3, \ldots, l^*$, où s est dans l'exposant symbolique la substitution $s = (\zeta : \zeta^r)$.

L'unité η_1, $(l-1)^{\text{ième}}$ puissance d'un entier de $c(\zeta)$, est nécessairement $\equiv 1$, mod $\mathfrak{l}$, et il en est alors de même de chacune des unités ε_t.

Supposons formés conformément au paragraphe 131 les polynômes adjoints $\varepsilon_t(x)$ pour chaque unité ε_t : on a pour les nombres rationnels

$$l^{(1)}(\varepsilon_t), \quad l^{(2)}(\varepsilon_t), \quad \ldots, \quad l^{(l-2)}(\varepsilon_t),$$

c'est-à-dire, pour les valeurs des $l-2$ premières dérivées du logarithme de $\varepsilon_t(e^v)$ pour $v = 0$, les congruences

(110)
$$\begin{cases} l^{(u)}(\varepsilon_t) \equiv 0, & (\text{mod } l), \\ \quad {\scriptstyle (u = 1, 2, 3, \ldots, 2t-1, 2t+1, \ldots, l-3, l-2)} & \\ l^{(2t)}(\varepsilon_t) \equiv (-1)^{t+1} \dfrac{B_t}{4tr^{2t}}, & (\text{mod } l). \\ \quad {\scriptstyle (t = 1, 2, \ldots, l^*)} & \end{cases}$$

Pour le démontrer, observons que d'après la première formule $(81)'$, paragraphe 131, on peut, dans le calcul des $l-2$ premières dérivées

$$l^{(1)}(\eta_1), \quad l^{(2)}(\eta_1), \quad \ldots, \quad l^{(l-2)}(\eta_1),$$

relatives au nombre η_1, prendre directement, au lieu du polynôme adjoint à η_1, le polynôme suivant :

$$\eta_1(x) = \left(\frac{(1-x^r)(1-x^{-r})}{(1-x)(1-x^{-1})}\right)^{\frac{l-1}{2}}.$$

Puis on a le développement connu

$$\log \frac{e^v - 1}{v} = + \frac{1}{2} v + \frac{B_1 \cdot v^2}{2 \cdot 2!} - \frac{B_2}{4 \cdot 4!} v^4 + \frac{B_3}{6 \cdot 6!} v^6 - \ldots,$$

où B_1, B_2, B_3, ... sont les nombres de Bernoulli.

De ce développement, résulte

$$(111) \qquad \log \tilde{\eta}_1(e^v) = (l-1) \Big\{ \log r + (r^2 - 1) \frac{B_1}{2 \cdot 2!} v^2 - (r^4 - 1) \frac{B_2}{4 \cdot 4!} v^4 + (r^6 - 1) \frac{B_3}{6 \cdot 6!} v^6 - \ldots \Big\}.$$

Les fonctions $\tilde{\eta}_1(e^{rv})$, $\tilde{\eta}_1(e^{r^2 v})$, ... jouent le même rôle par rapport aux nombres $s\eta_1$, $s^2\eta_1$, ... que $\tilde{\eta}_1(e^v)$ par rapport à η_1. En remplaçant alors dans l'expression (109) de ε_t, η_1, $s\eta_1$, $s^2\eta_1$ ... par $\tilde{\eta}_1(e^v)$, $\tilde{\eta}_1(e^{rv})$, $\tilde{\eta}_1(e^{r^2 v})$, on obtient une fonction $\tilde{\varepsilon}_t(e^v)$, qui peut tenir lieu de la fonction $\varepsilon_t(e^v)$ pour le calcul de $l^{(1)}(\varepsilon_t)$, $l^{(2)}(\varepsilon_t)$, ..., $l^{(l-2)}(\varepsilon_t)$. De (111) on tire (¹)

$$\log \tilde{\varepsilon}_t(e^v) = (l-1) \Big\{ C + (-1)^t (r^2 - r^{2t})(r^4 - r^{2t}) \ldots$$
$$\ldots (r^{2t-2} - r^{2t})(r^{2t+2} - r^{2t})(r^{2t+4} - r^{2t}) \ldots (r^{l-3} - r^{2t})(1 - r^{2t}) \frac{B_t}{2t(2t)!} v^{2t} \Big\}$$
$$+ C_{l-1} v^{l-1} + C_{l+1} v^{l+1} + \ldots,$$

où C, C_{l-1}, C_{l+1}, ..., désignent certaines constantes. Le produit écrit en détail dans le coefficient de v^{2t} est

$$(-1)^{l^*} \left[\frac{d(x-1)(x-r^2)\ldots(x-r^{l-3})}{dx} \right]_{(x=r^{2t})}$$

et le polynôme à dériver ci-dessus est $\equiv x^{\frac{l-1}{2}} - 1$, mod l. Le développement ci-dessus entraîne immédiatement les congruences (110).

Comme par hypothèse les numérateurs des l^* premiers nombres de Bernoulli B_1, ..., B_{l^*} ne sont pas divisibles par l, les l^* dérivées $l^{(2t)}(\varepsilon_t)$ pour $t = 1, 2, \ldots, l^*$ sont

---

(¹) N. T. — En représentant, en effet, l'exposant de η_1 dans ε_t par $f(s) = a_0 + a_1 s + \ldots + a_{l^*-1} s^{l^*-1}$, on a $f(r^{2u}) = 0$ pour $u = 1, 2, \ldots, t-1, t+1, \ldots, l^*$. De sorte que, vu

$$\log \tilde{e}(e^v) = a_0 \log \tilde{\eta}_1(e^v) + a_1 \log \tilde{\eta}_1(e^{rv}) + \ldots + a_{l^*-1} \log \tilde{\eta}_1(e^{r^{l^*-1} v}),$$

on a pour coefficient de v^{2u}

$$(r^{2u} - 1) \frac{B_u}{2u \cdot 2u!} f(r^{2u}),$$

c'est-à-dire o pour les valeurs de u de 1 à l^*, à l'exception de $u = t$.

toutes $\not\equiv 0$, mod l, d'après (110). Nous en concluons qu'aucune des unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ n'est $\equiv 1$, mod l. En posant alors

$$(112) \qquad \begin{cases} \varepsilon_1 \equiv 1 + a_1 \lambda^{e_1}, & (\mathfrak{l}^{e_1+1}), \\ \cdots\cdots\cdots\cdots \\ \varepsilon_{l^*} \equiv 1 + a_{l^*} \lambda^{e_{l^*}}, & (\mathfrak{l}^{e_{l^*}+1}) \end{cases}$$

avec des exposants $e_1, \ldots, e_{l^*}$ tels que $a_1, \ldots, a_{l^*}$ soient des entiers non divisibles par l, ces exposants $e_1, \ldots, e_{l^*}$ sont tous $< l - 1$. Puis on tire des congruences (112), le développement d'une expression $(1 - e^v)^g$ suivant les puissances de v commençant par le terme $(-1)^g v^g$, les congruences suivantes pour l'unité ε_t :

$$l^{(1)}(\varepsilon_t) \equiv 0, \quad l^{(2)}(\varepsilon_t) \equiv 0, \quad \ldots, \quad l^{(e_t - 1)}(\varepsilon_t) \equiv 0, \quad (\text{mod } l),$$
$$l^{(e_t)}(\varepsilon_t) \equiv (-1)^{e_t} a_t . e_t ! , \qquad (\text{mod } l),$$

et comme a_t ne doit pas être divisible par l, on tire des congruences (110), vu la remarque faite plus haut, $e_t = 2t$, ce qui démontre le lemme 29.

§ 139. — Critérium pour les nombres premiers réguliers.

Voici un critérium simple pour les nombres premiers réguliers l.

Théorème 154. — Pour qu'un nombre premier l soit régulier, il faut et il suffit qu'il ne divise le numérateur d'aucun des $l^* = \frac{l-3}{2}$ premiers nombres de Bernoulli. [Kummer[8].]

Démonstration. — Le lemme 28 montre que, si l divise le numérateur d'un des l^* premiers nombres de Bernoulli, l divise aussi le nombre de classes h du corps $c(\zeta)$. Dans le cas contraire, l est, toujours d'après ce lemme, premier au premier facteur du nombre de classes. Il y a donc encore seulement à démontrer que le second facteur du nombre de classes h n'est pas non plus divisible par l lorsque l'un des l^* premiers nombres de Bernoulli ne l'est pas.

Soit $\eta_1, \ldots, \eta_{l^*}$ un système de l^* unités réelles de $c(\zeta)$, système qui existe toujours d'après le théorème 127; nous pouvons alors poser

$$(113) \qquad s^t \varepsilon = \eta_1^{m_{1t}} \eta_2^{m_{2t}} \cdots \eta_{l^*}^{m_{l^*t}},$$

pour $t = 0, 1, 2, \ldots, l^* - 1$, les exposants $m_{1t}, m_{2t}, \ldots, m_{l^*t}$ étant des entiers rationnels et ε l'unité circulaire définie formule (108). On tire de (113)

$$(114) \qquad \log |s^t \varepsilon| = m_{1t} \log |\eta_1| + m_{2t} \log |\eta_2| + \ldots + m_{l^*t} \log |\eta_{l^*}|$$

pour $t = 0, 1, 2, \ldots, l^* - 1$, log représentant la partie réelle du logarithme. D'autre part, les égalités (109) définissant les unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ entraînent un système de la forme

$$(115) \qquad \varepsilon_t = \varepsilon^{n_{1t}}(s\varepsilon)^{n_{2t}}\ldots(s^{l^*-1}\varepsilon)^{n_{l^*t}}. \qquad (t = 1, 2, \ldots, l^*)$$

Nous en tirons les égalités

$$(116) \qquad \log \varepsilon_t = n_{1t}\log|\varepsilon| + n_{2t}\log|s\varepsilon| + \ldots + n_{l^*t}\log|s^{l^*-1}\varepsilon|, \qquad (t = 1, 2, \ldots, l^*)$$

et ensuite, à cause de (114),

$$(117) \qquad \log \varepsilon_t = \mathrm{M}_{1t}\log|\eta_1| + \mathrm{M}_{2t}\log|\eta_2| + \ldots + \mathrm{M}_{l^*t}\log|\eta_{l^*}|, \qquad (t = 1, 2, \ldots, l^*)$$

où $\mathrm{M}_{1t}, \mathrm{M}_{2t}, \ldots, \mathrm{M}_{l^*t}$ sont les combinaisons bilinéaires connues des $2l^{*2}$ entiers $n_{11}, n_{21}, \ldots, n_{l^*l^*}$; $m_{10}, m_{20}, \ldots, m_{l^*l^*}$. Les systèmes (113) et (115) en donnent encore chacun $l^* - 1$, si l'on effectue sur les unités qui y figurent les substitutions $s, s^2, \ldots, s^{l^*-1}$. En prenant les logarithmes, nous passons de même aux systèmes correspondant à (114), (116) et (117).

En posant alors

$$\mathrm{R} = \begin{vmatrix} \log|\eta_1|, & \ldots, & \log|\eta_{l^*}| \\ \log|s\eta_1|, & \ldots, & \log|s\eta_{l^*}| \\ \ldots & \ldots & \ldots \\ \log|s^{l^*-1}\eta_1|, & \ldots, & \log|s^{l^*-1}\eta_{l^*}| \end{vmatrix},$$

$$\Delta = \begin{vmatrix} \log|\varepsilon|, & \log|s\varepsilon|, & \ldots, & \log|s^{l^*-1}\varepsilon| \\ \log|s\varepsilon|, & \log|s^2\varepsilon|, & \ldots, & \log|s^{l^*}\varepsilon| \\ \ldots & \ldots & \ldots & \ldots \\ \log|s^{l^*-1}\varepsilon|, & \log|s^{l^*}\varepsilon|, & \ldots, & \log|s^{2l^*-2}\varepsilon| \end{vmatrix},$$

$$\overline{\Delta} = \begin{vmatrix} \log \varepsilon_1, & \log \varepsilon_2, & \ldots, & \log \varepsilon_{l^*} \\ \log s\varepsilon_1, & \log s\varepsilon_2, & \ldots, & \log s\varepsilon_{l^*} \\ \ldots & \ldots & \ldots & \ldots \\ \log s^{l^*-1}\varepsilon_1, & \log s^{l^*-1}\varepsilon_2, & \ldots, & \log s^{l^*-1}\varepsilon_{l^*} \end{vmatrix},$$

on trouve, par la règle de multiplication des déterminants,

$$(118) \qquad \frac{\overline{\Delta}}{\mathrm{R}} = \frac{\overline{\Delta}}{\Delta}\cdot\frac{\Delta}{\mathrm{R}} = \begin{vmatrix} \mathrm{M}_{11}, & \mathrm{M}_{21}, & \ldots, & \mathrm{M}_{l^*1} \\ \mathrm{M}_{12}, & \mathrm{M}_{22}, & \ldots, & \mathrm{M}_{l^*2} \\ \ldots & \ldots & \ldots & \ldots \\ \mathrm{M}_{1l^*}, & \mathrm{M}_{2l^*}, & \ldots, & \mathrm{M}_{l^*l^*} \end{vmatrix}.$$

Le déterminant du second membre est un entier rationnel et il n'est pas divisible par l. Car, dans le cas contraire, on pourrait trouver l^* entiers $N_1, \ldots, N_{l^*}$, non tous divisibles par l et rendant divisibles par l toutes les sommes

$$\sum_{(i)} N_i M_{1i}, \quad \sum_{(i)} N_i M_{2i}, \quad \ldots, \quad \sum_{(i)} N_i M_{l^* i} \qquad (i = 1, 2, \ldots, l^*).$$

On obtiendrait alors, vu (117), une égalité de la forme

$$N_1 \log \varepsilon_1 + N_2 \log \varepsilon_2 + \ldots + N_{l^*} \log \varepsilon_{l^*} = l . \log \mathsf{E},$$

où E serait une certaine unité positive de $c(\zeta)$. D'où

$$(119) \qquad \varepsilon_1^{N_1} \varepsilon_2^{N_2} \ldots \varepsilon_{l^*}^{N_{l^*}} = \mathsf{E}^l.$$

Mais une telle égalité est impossible. Car on en tirerait d'abord $\mathsf{E} \equiv \mathsf{E}^l \equiv 1$, mod $\mathfrak{l}$; en considérant le polynôme adjoint $\mathsf{E}(x)$ et les valeurs pour $v = 0$ des $l - 2$ premières dérivées de $\log \mathsf{E}(e^v)$, on déduirait de (119), en appliquant (110) les congruences

$$(-1)^{i-1} \frac{B_i}{4ir^{2i}} N_i \equiv 0, \quad (\text{mod } l), \qquad (i = 1, 2, \ldots, l^*)$$

Mais tous les nombres de Bernoulli $B_1, \ldots, B_{l^*}$ doivent être premiers à l, tandis que les nombres $N_1, \ldots, N_{l^*}$ ne sont pas tous divisibles par l; il y a donc contradiction.

Ainsi le déterminant du second membre de (118) n'est pas divisible par l. Comme, d'autre part, les facteurs $\frac{\bar{\Delta}}{\Delta}$ et $\frac{\Delta}{R}$ sont toujours entiers et que $\frac{\Delta}{R}$ représente le second facteur du nombre de classes h, le second facteur du nombre de classes n'est donc pas non plus divisible par l. Le théorème 154 est ainsi complètement démontré.

En s'appuyant sur ce théorème, on voit, d'après les valeurs des 47 premiers nombres de Bernoulli, qu'en dehors de 37, 59 et 67 tous les nombres premiers inférieurs à 100 sont réguliers. Le calcul montre, d'ailleurs, que les nombres de classes h relatifs aux corps $c\left(e^{\frac{2i\pi}{l}}\right)$ pour $l = 37$, 59 et 67 ne sont divisibles que par l et non par l^2. [Kummer [11, 26].]

§ 140. — Système particulier d'unités indépendantes d'un corps circulaire régulier.

Le paragraphe 139 nous fournit le moyen de déterminer dans un corps circulaire régulier un système d'unités qui nous sera utile dans la suite.

Théorème 155. — *l étant un nombre premier régulier, il existe toujours dans le*

corps circulaire $c\left(e^{\frac{2i\pi}{l}}\right)$ un système de $l^* = \frac{l-3}{2}$ unités indépendantes, $\bar\varepsilon_1, \ldots, \bar\varepsilon_{l^*}$ vérifiant les congruences

$$\bar\varepsilon_1 \equiv 1 + \lambda^2, \quad (\mathfrak{l}^3),$$
$$\bar\varepsilon_2 \equiv 1 + \lambda^4, \quad (\mathfrak{l}^5),$$
$$\ldots\ldots\ldots$$
$$\bar\varepsilon_{l^*} \equiv 1 + \lambda^{l-3}, \quad (\mathfrak{l}^{l-2}),$$

$(\lambda = 1 - \zeta,\ \mathfrak{l} = (1 - \zeta))$.

Démonstration. — $c(\zeta)$ étant régulier, les numérateurs des l^* premiers nombres de Bernoulli sont tous premiers à l, et il existe par suite (lemme 29) l^* unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ vérifiant les congruences (107). Comme $a_1, \ldots, a_{l^*}$ sont premiers à l, nous pouvons déterminer l^* entiers $b_1, \ldots, b_{l^*}$ tels que l'on ait

$$a_1 b_1 \equiv 1, \quad \ldots, \quad a_{l^*} b_{l^*} \equiv 1, \quad (\mathrm{mod}\ l).$$

En posant alors

$$\bar\varepsilon_1 = \varepsilon_1^{b_1}, \quad \ldots, \quad \bar\varepsilon_{l^*} = \varepsilon_{l^*}^{b_{l^*}},$$

les unités $\bar\varepsilon_1, \ldots, \bar\varepsilon_{l^*}$ vérifient les congruences du théorème 155.

De plus, elles forment un système d'unités indépendantes, parce que les unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ du paragraphe 138 en forment un. Pour montrer ce dernier point, supposons au contraire qu'il existe une égalité

(120) $$\bar\varepsilon_1^{e_1} \cdots \bar\varepsilon_{l^*}^{e_{l^*}} = 1,$$

les exposants étant des entiers non tous nuls; on peut supposer ensuite que ces exposants ne sont pas tous divisibles par l, car, dans le cas contraire, on aurait

$$\bar\varepsilon_1^{\frac{e_1}{l}} \cdots \bar\varepsilon_{l^*}^{\frac{e_{l^*}}{l}} = 1.$$

Ces exposants n'étant pas tous divisibles par l, l'équation 120 serait de la même forme que (119) qui a été déjà reconnue impossible au paragraphe 139.

§ 141. Propriété caractéristique des unités d'un corps circulaire régulier.

Théorème 156. — l étant un nombre premier régulier, s'il existe dans le corps $c\left(e^{\frac{2i\pi}{l}}\right)$ une unité E congrue mod l à un entier rationnel, elle est nécessairement égale à la $l^{\text{ième}}$ puissance d'une unité de ce corps. [Kummer[8].]

Démonstration. — Supposons déterminé un système d'unités $\bar\varepsilon_1, \ldots, \bar\varepsilon_{l^*}$ conformément au théorème 155; comme elles sont indépendantes, on a

(121) $$\mathsf{E}^{e} = \bar\varepsilon_1^{e_1} \cdots \bar\varepsilon_{l^*}^{e_{l^*}},$$

$e, e_1, \ldots, e_{l^*}$ étant des entiers rationnels non tous nuls, et l'on voit de suite qu'ils peuvent aussi être supposés non tous $\equiv 0$, mod l(1). Alors si e était divisible par l, l'égalité (121) serait de la forme (119), qui est impossible. Si, au contraire, e n'était pas divisible par l, on aurait $\mathsf{E}^e \equiv 1$, mod $\mathfrak{l}$, et, par suite, $\equiv 1$, mod l; prenons alors la dérivée logarithmique des polynômes adjoints des deux membres de (121). Comme E^e étant $\equiv 1$, mod l, les nombres $l^{(g)}(\mathsf{E}^e)$ sont tous $\equiv 0$, mod l pour $g \leq l-1$, il en résulte, en prenant $g = 2, 4, \ldots, 2l^*$, et tenant compte des valeurs des nombres $l^{(g)}(\varepsilon_1), \ldots, l^{(g)}(\varepsilon_{l^*})$, et de (110), que l'on a successivement $e_1 \equiv 0, \ldots, e_{l^*} \equiv 0$, mod l; on a donc $\mathsf{E}^e = \mathsf{H}^l$, H étant une certaine unité du corps, e n'étant pas divisible par l. En déterminant alors deux nombres a et b, tels que $ae + bl = 1$, on a

$$\mathsf{E} = (\mathsf{H}^a \mathsf{E}^b)^l,$$

ce qui démontre le théorème 156.

On est conduit par les considérations suivantes à une démonstration tout à fait différente de ce théorème.

Si E n'était pas égale à la $l^{\text{ème}}$ puissance d'une unité de $c(\zeta)$, $\mathsf{H} = \mathsf{E}^{1-s}$ ne pourrait l'être non plus; car $1 - s$ et $1 + s + \ldots + s^{l-2}$ sont deux polynômes à coefficients entiers en s sans diviseur commun mod l. Mais si E est congru mod l à un entier rationnel, on a $\mathsf{H} \equiv 1$, mod $\mathfrak{l}^l$, ce qui, vu la deuxième partie du théorème 148, exigerait que le corps kummerien $c(\sqrt[l]{\mathsf{H}}, \zeta)$ ait le discriminant relatif 1 par rapport à $c(\zeta)$. Mais comme ce corps kummerien est abélien relatif de degré relatif l par rapport à $c(\zeta)$, le théorème 94 exigerait que le nombre des classes d'idéaux du corps circulaire $c(\zeta)$ fût divisible par l, contrairement à l'hypothèse qu'il est régulier.

§ 142. — Nombres primaires d'un corps circulaire régulier.

Un entier α du corps circulaire régulier $c(\zeta)$ est dit *primaire* : 1° s'il est semi-primaire (voir § 115) et 2° si le carré de son module, c'est-à-dire son produit par le nombre imaginaire conjugué $s^{\frac{l-1}{2}}\alpha$, est congru à un entier rationnel mod $\mathfrak{l}^{l-1} = l$. Un nombre primaire est donc toujours premier à $\mathfrak{l}$ et vérifie les congruences

$$\alpha \equiv a, \quad (\mathfrak{l}^2),$$

$$\alpha \cdot s^{\frac{l-1}{2}}\alpha \equiv b, \quad (\mathfrak{l}^{l-1}),$$

a et b étant des entiers rationnels. [Kummer [12].]

---

(1) N. T. — En effet, dans le cas contraire, en extrayant la racine $l^{\text{ème}}$, on aurait $\mathsf{E}^{e'} = \zeta^k \varepsilon_1^{e'_1} \ldots \varepsilon_{l^*}^{e'_{l^*}}$, et $\mathsf{E}^{e'}$ étant congrue, mod l, à un entier rationnel, et les unités ε_a étant réelles, on aurait, la congruence devant subsister quand on change ζ en ζ^{-1},

$$\zeta^{k} \equiv \zeta^{-k}, \qquad (\text{mod } l),$$

c'est-à-dire $k \equiv 0$, (mod l), et en continuant ainsi, tant que les exposants sont tous divisibles par l, on arrive bien finalement à une égalité (121).

Théorème 157. — Dans un corps circulaire régulier $c(\zeta)$, on obtient un nombre primaire en multipliant un entier quelconque premier à $\mathfrak{l}$ par une unité convenable. [Kummer[12].]

Démonstration. — Le nombre $\beta = \alpha . s^{\frac{l-1}{2}} \alpha$ est évidemment un nombre du sous-corps de degré $\frac{l-1}{2}$ du corps $c(\zeta)$ et vérifie par suite une congruence $\beta \equiv a$, mod $\mathfrak{l}^2$, a étant un entier rationnel non divisible par l. Soient $\bar{\varepsilon}_1, \bar{\varepsilon}_2, \ldots, \bar{\varepsilon}_{l^*}$ les l^* unités du paragraphe 140. Si on a, par exemple, $\beta \equiv a + a_1\lambda^2$, mod $\mathfrak{l}^4$, a_1 étant un entier rationnel, on déterminera un entier rationnel u_1, tel que l'on ait $2au_1 + a_1 \equiv 0$, mod l; alors on a nécessairement

$$\beta\bar{\varepsilon}_1^{2u_1} \equiv a, \quad (\mathfrak{l}^4).$$

Si l'on a ensuite, par exemple, $\beta\bar{\varepsilon}_1^{2u_1} \equiv a + a_2\lambda^4$, mod $(\mathfrak{l}^6)$, a_2 étant un entier rationnel, on déterminera un entier u_2, tel que l'on ait $2au_2 + a_2 \equiv 0$, mod l; on a dès lors

$$\beta\bar{\varepsilon}_1^{2u_1}\bar{\varepsilon}_2^{2u_2} \equiv a, \quad (\mathfrak{l}^6).$$

On arrive finalement à

$$\beta\bar{\varepsilon}_1^{2u_1}\bar{\varepsilon}_2^{2u_2}\ldots\bar{\varepsilon}_{l^*}^{2u_{l^*}} = \beta\bar{\varepsilon}^2 \equiv a, \quad (\text{mod } \mathfrak{l}^{l-1}).$$

Si, d'autre part, ζ^* est une puissance de ζ telle que $\zeta^*\alpha$ soit semi-primaire, $\zeta^*\bar{\varepsilon}\alpha$ sera évidemment primaire.

Un nombre primaire réel est toujours congru, mod $l = \mathfrak{l}^{l-1}$, à un entier rationnel. D'après le théorème 156, toute unité primaire de $c(\zeta)$ est la $l^{\text{ième}}$ puissance d'une unité de $c(\zeta)$.

Voici encore un lemme sur les nombres primaires qui sera utile dans la suite.

Lemme 30. — ν, μ étant deux nombres primaires du corps circulaire régulier $c(\zeta)$, on a toujours $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1$.

Démonstration. — Nous pouvons supposer les deux nombres $\nu, \mu \equiv 1$, mod $\mathfrak{l}$, car autrement leurs $(l-1)^{\text{ièmes}}$ puissances rempliraient sûrement cette condition, et à cause de $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1}, \mu^{l-1}}{\mathfrak{l}}\right\}$ (voir § 131), on pourrait les substituer à ν et μ. D'après (83), on a

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu, s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu . s^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right\},$$

et comme par hypothèse on a $\mu . s^{\frac{l-1}{2}}\mu \equiv 1$, mod $\mathfrak{l}^{l-1}$, et que $\nu \equiv 1$, mod $\mathfrak{l}^2$, on tire

immédiatement de la définition générale (82) du symbole $\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right) : \left(\frac{\nu,\,\mu\,.\,S^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right) = 1$, et, par suite,

$$\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right)\left(\frac{\nu,\,S^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right) = 1.$$

On démontre de même que

$$\left(\frac{\nu,\,S^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right)\left(\frac{S^{\frac{l-1}{2}}\nu,\,S^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right) = 1.$$

Puis de la formule (84) on tire

$$\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right)\left(\frac{S^{\frac{l-1}{2}}\nu,\,S^{\frac{l-1}{2}}\mu}{\mathfrak{l}}\right) = 1.$$

Les trois dernières égalités donnent

$$\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right)^2 = 1, \quad \text{c.-à-d.} \quad \left(\frac{\nu,\,\mu}{\mathfrak{l}}\right) = 1. \qquad \text{C. q. f. d.}$$

CHAPITRE XXXII.

Classes d'idéaux invariantes [1] et genres d'un corps kummerien régulier.

§ 143. — Familles d'unités d'un corps circulaire régulier.

Soit l un nombre premier impair régulier, et considérons dans le corps circulaire régulier $c\left(\zeta = e^{\frac{2i\pi}{l}}\right)$ un ensemble E d'unités contenant les $l^{\text{ièmes}}$ puissances de toutes les unités du corps et tel, de plus, que le produit et le quotient de deux unités quelconques de l'ensemble en fasse encore partie. On appellera un tel ensemble une *famille d'unités du corps circulaire* $c(\zeta)$.

Dans toute famille, on peut déterminer m unités $\varepsilon_1, \ldots, \varepsilon_m$ telles que toute unité de la famille est représentée une fois et une seule par l'expression

$$\varepsilon_1^{u_1}\varepsilon_2^{u_2}\ldots\varepsilon_m^{u_m}\xi^l$$

lorsqu'on donne à chacun des exposants $u_1, \ldots, u_m$, les valeurs $0, 1, \ldots, l-1$ et où ξ est une unité quelconque de $c(\zeta)$. J'appellerai un tel système $\varepsilon_1, \ldots, \varepsilon_m$ *base de la famille*. Il est clair qu'on ne peut avoir

$$\varepsilon_1^{e_1}\ldots\varepsilon_m^{e_m} = \xi^l,$$

(1) Ou *ambiges*.

$e_1, \ldots, e_l$ étant des entiers rationnels non tous divisibles par l et ε une unité de $c(\zeta)$. On voit aisément que toute autre base de la famille E comprend le même nombre m d'unités ; ce nombre m s'appellera *le degré de la famille d'unités*.

Si, en particulier, une famille d'unités ne contient que les $l^{\text{ièmes}}$ puissances d'unités de $c(\zeta)$, elle contient le plus petit nombre possible d'unités et son degré est o. La totalité des unités de $c(\zeta)$ est aussi une famille d'unités ; toute unité de $c(\zeta)$ est (théorème 127) le produit d'une racine $l^{\text{ième}}$ de l'unité et d'une unité réelle : on conclut de là et des développements de la démonstration du théorème 157 que les unités $\bar{\varepsilon}_1$, ..., $\bar{\varepsilon}_{\frac{l-3}{2}}$ du paragraphe 140 forment avec ζ une base de cette famille d'unités, qui est la plus étendue. Son degré est donc $\frac{l-1}{2}$; c'est évidemment la seule famille de degré $\frac{l-1}{2}$ et il n'y en a pas de degré plus élevé.

On voit facilement que les normes relatives de toutes les unités d'un corps kummerien $c(\sqrt[l]{\mu}, \zeta)$ déduit de $c(\zeta)$ forment une famille d'unités de $c(\zeta)$; enfin, la totalité des unités égales à des normes relatives, soit d'unités, soit de fractions du corps kummerien $c(\sqrt[l]{\mu}, \zeta)$, forment une famille d'unités de $c(\zeta)$.

§ 144. — Idéaux invariants (1), classes d'idéaux invariantes (1) d'un corps kummerien régulier.

Soit $c(\zeta)$ un corps circulaire régulier, μ un entier de $c(\zeta)$, qui ne soit pas puissance $l^{\text{ème}}$ d'un nombre de $c(\zeta)$; soit C le corps kummerien régulier $c(\mathsf{M}, \zeta)$ engendré par $\mathsf{M} = \sqrt[l]{\mu}$ et ζ. Cherchons maintenant à développer la théorie de ce corps par des méthodes correspondant à celles qu'on a employées pour le corps quadratique dans les chapitres XVII et XVIII.

Le groupe relatif de C par rapport à $c(\zeta)$ est formé de puissances de la substitution $S = (\mathsf{M} : \zeta\mathsf{M})$; on appellera, d'après le paragraphe 57, un idéal $\mathfrak{A}$ de C *idéal invariant* (1), quand la substitution S le laissera invariant, $S\mathfrak{A} = \mathfrak{A}$, et que, de plus, $\mathfrak{A}$ ne contiendra en facteurs aucun idéal de $c(\zeta)$ différant de 1.

D'après le théorème 93, les idéaux premiers qui divisent le discriminant relatif de C sont tous invariants, et il n'y a pas d'autres idéaux invariants. $\mathfrak{A}$ étant donc un

---

(1) L'expression de M. Hilbert est *ambig*. Selon une remarque de M. E. Cahen, l'origine de ce mot remonte à la traduction, par Poulet-Delisle, des *Disquisitiones arithmeticae* : il traduit par *ambigu* le mot *anceps*, employé par Gauss dans sa théorie des formes quadratiques. M. Lévy, vu l'acception habituelle différente du mot *ambigu*, a employé le mot *ambige* dans ses traductions de l'ouvrage de Sommer et des trois premières parties de l'ouvrage actuel. M. de la Vallée-Poussin emploie le mot *bilatère*. Je propose *invariant*, qui a l'avantage de rappeler la définition des classes dont il s'agit.

idéal invariant quelconque de C, nous déduisons facilement de $S\mathfrak{A} = \mathfrak{A}$ (voir § 73) que tout idéal premier de C qui divise $\mathfrak{A}$ doit aussi être invariant, et il en résulte que le nombre de tous les idéaux invariants est l^t.

$\mathfrak{K}$ étant un idéal d'une classe K du corps de Kummer C, la classe d'idéaux déterminée par l'idéal conjugué relatif $S\mathfrak{K}$ sera représentée par SK. Les classes SK, S^2K, ..., $S^{l-1}K$ s'appelleront les *classes conjuguées relatives de* K. F(S) étant un polynôme quelconque de degré $l-1$ en S à coefficients $a, a_1, \ldots, a_{l-1}$ entiers rationnels :

$$F(S) = a + a_1 S + \ldots + a_{l-1} S^{l-1}$$

la classe déterminée par l'expression

$$K^a (SK)^{a_1} (S^2 K)^{a_2} \ldots (S^{l-1} K)^{a_{l-1}},$$

s'appellera la *puissance symbolique* F(S) de la classe K et se représentera par

$$K^{a + a_1 S + a_2 S^2 + \ldots + a_{l-1} S^{l-1}} = K^{F(S)}.$$

Enfin, une classe d'idéaux A du corps kummerien sera dite *classe ambige ou invariante* lorsqu'on aura $A = SA$, c'est-à-dire $A^{1-S} = 1$. La $l^{\text{ième}}$ puissance d'une classe ambige quelconque contient toujours parmi ses idéaux des idéaux de $c(\zeta)$. Cela résulte immédiatement de ce que l'on a

$$A^l = A^{1+S+S^2+\ldots+S^{l-1}},$$

à cause de $A = SA$ et que, d'autre part, la norme relative d'un idéal quelconque de C est un idéal de $c(\zeta)$.

§ 145. — Famille de classes dans un corps kummerien régulier.

Considérons dans le corps kummerien régulier C un ensemble de classes, tel que la $l^{\text{ième}}$ puissance de chacune d'elles contienne des idéaux de $c(\zeta)$ et que, de plus, il contienne toutes les classes contenant des idéaux de $c(\zeta)$; tel, de plus, que le produit et le quotient de deux classes de l'ensemble en fassent encore partie. J'appellerai un tel ensemble *une famille de classes du corps kummerien.* Dans toute famille de classes, on peut toujours déterminer n classes $K_1, \ldots, K_n$, telles que toute classe de la famille est représentée une fois, et une seule, par le produit

$$K_1^{u_1} K_2^{u_2} \ldots K_n^{u_n} k$$

lorsque $u_1, u_2, \ldots, u_n$ prennent séparément les valeurs 0, 1, ..., $l-1$, et k désignant une quelconque des classes renfermant parmi ses idéaux des idéaux de $c(\zeta)$. On appellera $K_1, \ldots, K_n$ *une base de la famille de classes.* On montre facilement que le nombre de classes de toute autre base de la famille est encore égal à n. Ce nombre n sera le *degré de la famille de classes.*

Si toutes les classes d'une famille contiennent des idéaux de $c(\zeta)$, elle est de degré o. Une autre famille de classes est encore formée par la totalité des classes de C contenant soit des idéaux invariants de C, soit des produits de tels idéaux par des idéaux de $c(\zeta)$. Enfin, la totalité des classes invariantes du corps kummerien forme une famille.

§ 146. — Deux lemmes généraux sur les unités fondamentales relatives d'un corps cyclique relatif de degré premier impair.

Avant de poursuivre les recherches du précédent paragraphe, établissons deux lemmes se rattachant au théorème 91 du paragraphe 55.

Lemme 31. — Soit l premier impair le degré relatif d'un corps C cyclique relatif par rapport à un sous-corps c, soit S une substitution autre que la substitution identique du groupe relatif de C par rapport à c, et soit $\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}$ un système d'unités fondamentales relatives du corps C par rapport à c; on a dès lors pour toute unité E de C une relation de la forme

$$\mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \cdots \mathsf{H}_{r+1}^{F_{r+1}(S)}[\varepsilon],$$

f étant un exposant entier rationnel non divisible par l, $F_1(S), \ldots, F_{r+1}(S)$ des polynômes entiers en S de degré $(l-2)$ à coefficients entiers et $[\varepsilon]$ une unité de C dont la $l^{\text{ième}}$ puissance appartient à c.

Démonstration. — De la démonstration du théorème 91 résulte que les unités

$$\mathsf{H}_1, \ldots, \mathsf{H}_{r+1}, S\mathsf{H}_1, \ldots, S\mathsf{H}_{r+1}, \ldots, S^{l-2}\mathsf{H}_1, \ldots, S^{l-2}\mathsf{H}_{r+1}$$

jointes à r unités fondamentales du corps c sont indépendantes, et comme il y en a en tout $l(r+1)-1$, il existe pour toute unité E de C des relations de la forme

$$(122) \qquad \mathsf{E}^{G(S)} = \mathsf{H}_1^{G_1(S)} \cdots \mathsf{H}_{r+1}^{G_{r+1}(S)}[\varepsilon],$$

où $G(S), G_1(S), \ldots, G_{r+1}(S)$ sont des polynômes entiers en S de degré $l-2$ à coefficients entiers, dont le premier n'est pas identiquement nul, et où $[\varepsilon]$ est une unité de C telle que $[\varepsilon]^l$ est dans c. Parmi les relations (122) en nombre infini, prenons-en une où $G(\zeta)$ soit divisible par une puissance de $1-\zeta$ aussi petite que possible. Admettons que ce soit précisément la relation (122); supposons, de plus, d'abord que $G(\zeta)$ soit au moins divisible par $1-\zeta$. D'après la définition des unités fondamentales, paragraphe 55, il faut que

$$G_1(\zeta), \ldots, G_{r+1}(\zeta)$$

soient aussi divisibles par $1-\zeta$. En élevant (122) à la puissance symbolique $(1-S^2)(1-S^3)\dots(1-S^{l-1})$ et en posant

$$G(\zeta)=(1-\zeta)G^*(\zeta),\quad G_1(\zeta)=(1-\zeta)G_1^*(\zeta),\quad \dots,$$

on trouve facilement, la $(1+S+S^2+\dots+S^{l-1})^{\text{ième}}$ puissance symbolique de toute unité de C étant dans c :

$$\text{(123)}\qquad \mathbf{E}^{lG^*(S)}=\mathbf{H}_1^{lG_1^*(S)}\dots\mathbf{H}_{r+1}^{lG_{r+1}^*(S)}[\varepsilon],$$

où $[\varepsilon]$ est encore une unité de c ou la racine $l^{\text{ième}}$ d'une unité de c.

A cause de l'égalité (123), une racine $l^{\text{ième}}$ de ce nombre $[\varepsilon]$ est certainement un nombre de C, et par suite aussi une unité de C dont la $l^{\text{ième}}$ puissance appartient à c, et qu'on désignera encore par $[\varepsilon]$; on tire alors de (123)

$$\mathbf{E}^{G^*(S)}=\mathbf{H}_1^{G_1^*(S)}\dots\mathbf{H}_{r+1}^{G_{r+1}^*(S)}[\varepsilon],$$

$[\varepsilon]$ étant encore une unité de C dont la $l^{\text{ième}}$ puissance est dans c. Cette égalité est de la même forme que (122), sauf que $G^*(\zeta)$ serait divisible par une puissance de $1-\zeta$ inférieure à celle qui divise $G(\zeta)$, ce qui est contradictoire à notre hypothèse sur le choix de (122). Donc $G(\zeta)$ ne peut être divisible par $1-\zeta$.

En posant $f=G(\zeta)G(\zeta^2)\dots G(\zeta^{l-1})$, f est un entier rationnel non divisible par l, et il existe évidemment deux polynômes entiers H(S), M(S) à coefficients entiers, vérifiant identiquement en S l'égalité

$$f=H(S)G(S)+M(S)(1+S+S^2+\dots+S^{l-1}).$$

En élevant (122) à la $H(S)^{\text{ième}}$ puissance symbolique on obtient la formule annoncée dans le lemme 31.

Lemme 32. — Conservons les mêmes notations que dans le lemme 31, prenons les normes relatives des $r+1$ unités fondamentales relatives du corps relatif cyclique C :

$$\eta_1=N_c(\mathbf{H}_1),\quad \dots,\quad \eta_{r+1}=N_c(\mathbf{H}_{r+1}),$$

toute unité ε de c égale à la norme relative d'une unité $\mathbf{E}$ de C est alors de la forme

$$\varepsilon=\eta_1^{u_1}\dots\eta_{r+1}^{u_{r+1}}[\varepsilon]^l,$$

$u_1, \dots, u_{r+1}$ étant des entiers rationnels et $[\varepsilon]$ une unité de C.

Démonstration. — D'après le lemme 31, nous avons pour $\mathbf{E}$ une égalité

$$\mathbf{E}^f=\mathbf{H}_1^{F_1(S)}\dots\mathbf{H}_{r+1}^{F_{r+1}(S)}[\varepsilon].$$

avec les notations de ce lemme. En prenant la norme relative par rapport à c, on obtient (1)

(24) $$\varepsilon^l = \eta_1^{F_1(1)} \ldots \eta_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(1)} [\varepsilon]^l.$$

En déterminant ensuite deux entiers rationnels a et b, tels que l'on ait $1 = af + bl$, et en élevant (24) à la puissance a, on obtient une formule conforme au lemme 32.

§ 147. — Les classes d'idéaux déterminées par les idéaux invariants.

Soit $C = c(\sqrt[l]{\mu}, \zeta)$ un corps kummerien régulier, prenons dans son groupe relatif la substitution $S = (\sqrt[l]{\mu} : \zeta\sqrt[l]{\mu})$. Comme tout idéal invariant $\mathfrak{A}$ de C détermine une classe invariante, vu $S\mathfrak{A} = \mathfrak{A}$, nous devons d'abord, pour arriver à la connaissance des classes invariantes, étudier la famille de classes engendrée par les idéaux invariants. On a l'importante proposition :

Théorème 158. — *Soit t le nombre des idéaux premiers distincts qui divisent le discriminant relatif du corps kummerien régulier $C = c(\sqrt[l]{\mu}, \zeta)$ de degré relatif l; les normes relatives de toutes les unités de C forment pour c une famille d'unités de degré m; si nous considérons alors toutes les classes contenant soit des idéaux invariants de C, soit des produits de tels idéaux par des idéaux de $c(\zeta)$, elles forment une famille de classes de degré*

$$t + m - \frac{l+1}{2}.$$

Démonstration. — Supposons d'abord que le nombre μ ne soit pas de la forme $\varepsilon\alpha^l$, où ε et α sont une unité et un nombre de $c(\zeta)$. Alors toute unité $[\varepsilon]$ du corps $C = c(\sqrt[l]{\mu}, \zeta)$ dont la $l^{\text{ème}}$ puissance est dans $c(\zeta)$ est nécessairement elle-même dans $c(\zeta)$; de plus, $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{l-1}{2}}$ désigneront un système d'unités fondamentales relatives du corps C par rapport à $c(\zeta)$ et

$$\eta_1 = N_c(\mathsf{H}_1), \quad \ldots, \quad \eta_{\frac{l-1}{2}} = N_c(\mathsf{H}_{\frac{l-1}{2}})$$

leurs normes relatives.

Nous prenons, *en premier lieu*, le cas extrême où l'on a $m = \frac{l-1}{2}$. Nous concluons du lemme 32 que les unités $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ forment une base de la famille

---

(1) N. T. — Si l'on a en effet

$$\Omega = \omega^{F(S)} = \omega^{a}(S\omega)^{a_1} \ldots (S^{l-2}\omega)^{a_{l-2}},$$

on en déduit

$$N_c(\Omega) = N_c(\omega)^{a} N_c(S\omega)^{a_1} \ldots [N_c(S^{l-2}\omega)]^{a_{l-2}} = [N_c(\omega)]^{a+a_1+\ldots+a_{l-2}} = [N_c(\omega)]^{F(1)}.$$

d'unités formée des normes relatives de toutes les unités de C. Considérons, d'autre part, les t idéaux premiers invariants $\mathfrak{L}_1, \ldots, \mathfrak{L}_t$ du corps C; ils déterminent t classes invariantes, que nous désignerons par $L_1, \ldots, L_t$. Pour déterminer le degré de la famille de classes qu'elles définissent, posons

$$(125) \qquad \mathsf{M} = \sqrt[l]{\mu} = \mathfrak{L}_1^{a_1} \ldots \mathfrak{L}_t^{a_t} \mathfrak{j},$$

où $a_1, \ldots, a_t$ sont des exposants entiers et $\mathfrak{j}$ un idéal de $c(\zeta)$. Vu l'hypothèse faite sur μ, l'un au moins des exposants $a_1, \ldots, a_t$ n'est pas divisible par l; soit, par exemple, a_t. Nous déduisons de (125) que

$$k = L_1^{a_1} \ldots L_t^{a_t}$$

est une classe contenant des idéaux du corps $c(\zeta)$; comme L_t^l est aussi une classe de cette espèce, il en résulte que L_t est le produit de puissances des classes $L_1, \ldots, L_{t-1}$ et d'une classe contenant des idéaux de $c(\zeta)$.

Démontrons maintenant que les classes $L_1, \ldots, L_{t-1}$ ne peuvent à elles seules composer aucune classe

$$(126) \qquad k' = L_1^{a'_1} \ldots L_{t-1}^{a'_{t-1}}$$

contenant des idéaux de $c(\zeta)$, à moins que tous les exposants $a'_1, \ldots, a'_{t-1}$ soient divisibles par l. En effet, de la relation (126) on tirerait une égalité

$$(127) \qquad \mathsf{M}' = \mathfrak{L}_1^{a'_1} \ldots \mathfrak{L}_{t-1}^{a'_{t-1}} \mathfrak{j}',$$

où $\mathfrak{j}'$ serait un idéal de $c(\zeta)$ et M' un entier de C; on en concluerait alors que $\mathsf{E} = \mathsf{M}'^{1-S}$ devrait être une unité de C. Appliquons à E le lemme 31; on a aussi une égalité de la forme

$$(128) \qquad \mathsf{E}^f = \mathsf{H}_1^{F_1(S)} \ldots \mathsf{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(S)} \varepsilon,$$

où f est un entier rationnel non divisible par l, $F_1(S), \ldots, F_{\frac{l-1}{2}}(S)$ des polynômes entiers en S à coefficients entiers et ε une unité de $c(\zeta)$. Comme on a évidemment $N_c(\mathsf{E}) = 1$, on a, en prenant la norme relative des deux membres de (128),

$$1 = \eta_1^{F_1(1)} \ldots \eta_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(1)},$$

$\eta_1, \ldots, \eta_{\frac{l-1}{2}}$ devant former la base d'une famille d'unités, les entiers $F_1(1), \ldots, F_{\frac{l-1}{2}}(1)$ doivent être tous divisibles par l, et par suite $F_1(\zeta), \ldots, F_{\frac{l-1}{2}}(\zeta)$ par $1-\zeta$. En posant

$$F_1(\zeta) = (1-\zeta) F_1(\zeta), \ \ldots, \ F_{\frac{l-1}{2}}(\zeta) = (1-\zeta) F_{\frac{l-1}{2}}(\zeta),$$

et

$$\mathsf{H}=\mathsf{H}_1^{F_1(S)}\cdots\mathsf{H}_{\frac{l-1}{2}}^{F_{\frac{l-1}{2}}(S)},$$

on a

$$\mathsf{E}^{l}=\mathsf{H}^{1-S}\varepsilon^{*},$$

ε^{*} étant encore une unité de $c(\zeta)$. Puis, en prenant la norme relative, on a $1=\varepsilon^{*l}$, c'est-à-dire que ε^{*} est une racine $l^{\text{ième}}$ de l'unité, par exemple $=\zeta^{g}$. Comme $\mathsf{M}^{1-S}=\zeta^{-1}$, on a

$$\{\mathsf{M}'^{f}\mathsf{M}^{g}\mathsf{H}^{-1}\}^{1-S}=1,$$

c'est-à-dire que l'expression $\mathsf{M}'^{f}\mathsf{M}^{g}\mathsf{H}^{-1}$ est un nombre de $c(\zeta)$. Comme M' (*voir* 127) ne contient pas l'idéal $\mathfrak{L}_t$ ou le contient à une puissance d'exposant divisible par l, que M contient, au contraire, $\mathfrak{L}_t$ à une puissance d'exposant a_t non divisible par l, la décomposition de ce nombre en idéaux premiers du corps $c(\zeta)$ montre d'abord que g doit être divisible par l; puis elle montre, f étant premier à l, que les exposants a_1', ..., a_{t-1}' devraient être tous divisibles par l, contrairement à l'hypothèse. Par conséquent il ne peut y avoir entre les classes L_1, ..., L_{t-1} une relation comme (126), c'est-à-dire que les classes L_1, ..., L_{t-1} forment, si $m=\frac{l-1}{2}$, une base de la famille de classes engendrée par la totalité des idéaux invariants; le degré de cette famille est donc $l-1-(l-m)=\frac{l+1}{2}$.

Supposons, *en second lieu*, $m=\frac{l-3}{2}$. Il doit alors exister entre les unités η_1, ..., $\eta_{\frac{l-1}{2}}$ une relation de la forme $\eta_1^{e_1}, \ldots, \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}}=\eta^{l}$, les exposants e_1, ..., $e_{\frac{l-1}{2}}$ n'étant pas tous divisibles par l, η étant une unité de $c(\zeta)$. Si $e_{\frac{l-1}{2}}$, par exemple, n'est pas divisible par l, η_1, ..., $\eta_{\frac{l-1}{2}}$ forment une base de la famille des normes relatives de toutes les unités de C : cela résulte du lemme 32. Formons alors l'unité

(129) $$\mathsf{E}=\mathsf{H}_1^{e_1}\cdots\mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}}\eta^{-1}.$$

Comme elle a pour norme relative 1, il existe dans C un entier Λ tel que l'on ait $\Lambda^{1-S}=\mathsf{E}$ (théorème 90). Déterminons — ce qui est toujours possible — un entier positif r tel que dans le produit $\mathsf{M}'=\Lambda\mathsf{M}^{r}$ l'idéal $\mathfrak{L}_t$ entre avec un exposant divisible par l. Les autres facteurs $\mathfrak{L}_1$, ..., $\mathfrak{L}_{t-1}$ ne pourront avoir tous dans M' des exposants divisibles par l, car autrement on aurait, d'après le théorème 153, $\mathsf{M}'=\Theta\alpha$, Θ étant une unité de C et α un entier de $c(\zeta)$; et on aurait par suite $\Theta^{1-S}=\mathsf{E}\zeta^{-r}$, contrairement à la définition (§ 55) des unités fondamentales relatives H_1, ..., $\mathsf{H}_{\frac{l-1}{2}}$, puisque, dans l'expression (129) de E, $e_{\frac{l-1}{2}}$ est premier à l. Alors l'idéal invariant $\mathfrak{L}_{t-1}$, par

exemple, entre dans M' avec un exposant non divisible par l. On en conclut que la classe L_{l-1} est le produit de puissances des classes $L_1, \ldots, L_{l-2}$ et d'une classe contenant des idéaux de $c(\zeta)$.

Démontrons maintenant que les classes $L_1, \ldots, L_{l-2}$ ne peuvent former aucune classe

(130) $$k'' = L_1^{a''_1} \ldots L_{l-2}^{a''_{l-2}}$$

contenant des idéaux de $c(\zeta)$, à moins que les exposants $a''_1, \ldots, a''_{l-2}$ soient tous divisibles par l.

En effet, une relation (130) entrainerait une égalité

(131) $$\mathsf{M}'' = \mathfrak{L}_1^{a''_1} \ldots \mathfrak{L}_{l-2}^{a''_{l-2}} \mathfrak{j}'',$$

M'' étant un entier de C et $\mathfrak{j}''$ un idéal de $c(\zeta)$; alors $\mathsf{E}' = \mathsf{M}''^{1-S}$ devrait être une unité de C. En lui appliquant le lemme 31, on obtient une égalité

(132) $$\mathsf{E}'^{f'} = \mathsf{H}_1^{F'_1(S)} \ldots \mathsf{H}_{\frac{l-1}{2}}^{F'_{\frac{l-1}{2}}(S)} \varepsilon,$$

f' étant un entier rationnel non divisible par l, les polynômes $F'(S)$ étant à coefficients entiers et ε une unité de $c(\zeta)$. Déterminons alors un exposant entier rationnel u tel que l'entier $F'_{\frac{l-1}{2}}(1) + ue_{\frac{l-1}{2}}$ soit divisible par l; on obtient, par rapport à $c(\zeta)$, comme $N_c(\mathsf{E}') = 1$,

(133) $$1 = \eta_1^{F'_1(1)+ue_1} \ldots \eta_{\frac{l-3}{2}}^{F'_{\frac{l-3}{2}}(1)+ue_{\frac{l-3}{2}}} \varepsilon'^{l},$$

ε' étant encore une unité de $c(\zeta)$. Les unités $\eta_1, \ldots, \eta_{\frac{l-3}{2}}$ étant une base d'une famille d'unités, il résulte de (133) que les exposants $F'_1(1) + ue_1, \ldots, F'_{\frac{l-3}{2}}(1) + ue_{\frac{l-3}{2}}$ sont tous divisibles par l, c'est-à-dire que tous les nombres

$$F'_1(\zeta) + ue_1, \quad \ldots, \quad F'_{\frac{l-3}{2}}(\zeta) + ue_{\frac{l-3}{2}}$$

sont divisibles par $1 - \zeta$. En posant

$$F'_1(\zeta) + ue_1 = (1-\zeta)F''_1(\zeta), \ \ldots, \ F'_{\frac{l-1}{2}}(\zeta) + ue_{\frac{l-1}{2}} = (1-\zeta)F''_{\frac{l-1}{2}}(\zeta)$$

et

$$\mathsf{H}' = \mathsf{H}_1^{F''_1(S)} \ldots \mathsf{H}_{\frac{l-1}{2}}^{F''_{\frac{l-1}{2}}(S)},$$

il résulte de (132)

$$\mathsf{E}'^{f'} \mathsf{E}^{u} = \mathsf{H}'^{1-S} \varepsilon'^{*},$$

où E est l'unité de C définie par (129) et ε'^{*} encore une unité de $c(\zeta)$; en prenant la

norme relative, on a $1 = \varepsilon'^{*l}$, c'est-à-dire que ε'^{*} est une racine de l'unité, égale par exemple à $\zeta^{g''}$. On a alors, en tenant compte des égalités :

$$\mathsf{M}^{1-S} = \zeta^{g-1}, \quad \mathsf{M}'^{1-S} = \mathsf{E}\zeta^{g'-r}, \quad \mathsf{M}''^{1-S} = \mathsf{E}',$$

$$\{\mathsf{M}''^{f'}\mathsf{M}'^{u}\mathsf{M}^{g'-ur}\mathsf{H}'^{\cdots}\}^{1-S} = 1,$$

c'est-à-dire que l'expression entre crochets est un nombre de $c(\zeta)$.

En remarquant que $\mathfrak{L}_l^l, \mathfrak{L}_{l-1}^l, \mathfrak{L}_{l-2}^l, \ldots, \mathfrak{L}_1^l$ sont idéaux premiers dans $c(\zeta)$, nous voyons d'abord que $g' - ur$ doit être divisible par l; alors, M' contenant par hypothèse l'idéal $\mathfrak{L}_{l-1}$ à une puissance d'exposant non multiple de l, tandis qu'au contraire M'' contient, d'après (131), $\mathfrak{L}_{l-1}$ à une puissance d'exposant multiple de l, on voit que u devrait aussi être divisible par l, et enfin, f' étant premier à l, que les exposants $a''_1, \ldots, a''_{l-2}$ devraient être tous divisibles par l, contrairement à l'hypothèse faite à leur sujet. Ainsi il est démontré qu'une relation (130) ne peut exister entre les $\mathrm{L}_1, \ldots, \mathrm{L}_{l-2}$, c'est-à-dire que ces classes forment dans le cas de $m = \frac{l-3}{2}$ une base de la famille de classes engendrée par tous les idéaux invariants; son degré est donc $l - 2$, conformément à la formule du théorème 158.

Supposons, *en troisième lieu*, $m = \frac{l-5}{2}$. Alors il existe entre les unités $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$, non seulement une relation de la forme $\eta_1^{e_1} \cdots \eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} = \eta^l$, η étant une unité de $c(\zeta)$ et l'un au moins des exposants, par exemple $e_{\frac{l-1}{2}}$ n'étant pas divisible par l; mais il y en a encore une de la forme $\eta_1^{e'_1} \cdots \eta_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} = \eta'^l$, η' étant encore une unité de $c(\zeta)$ et l'un des exposants e'_i, par exemple $e'_{\frac{l-3}{2}}$ n'étant pas divisible par l. Formons les unités

$$(134) \quad \begin{cases} \mathsf{E} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} \eta^{-1}, \\ \mathsf{E}' = \mathsf{H}_1^{e'_1} \cdots \mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \eta'^{-1}. \end{cases}$$

La norme relative de E et E' étant égale à 1, on peut (théorème 90) poser $\mathsf{E} = \mathsf{A}^{1-S}$ et $\mathsf{E}' = \mathsf{A}'^{1-S}$, A et A' étant des entiers de C. Si l'on détermine alors, comme dans le cas précédent, un entier positif r, tel que $\mathsf{M}' = \mathsf{A}\mathsf{M}^r$ contienne $\mathfrak{L}_l$ à une puissance d'exposant multiple de l, l'un au moins des facteurs $\mathfrak{L}_1, \ldots, \mathfrak{L}_{l-1}$ entre dans M' à une puissance d'exposant non multiple de l, soit par exemple $\mathfrak{L}_{l-1}$. Déterminons alors deux entiers positifs r' et r'' tels que $\mathsf{M}'' = \mathsf{A}'\mathsf{M}^{r'}\mathsf{M}'^{r''}$ contienne les deux facteurs $\mathfrak{L}_l$ et $\mathfrak{L}_{l-1}$ à des puissances d'exposants multiples de l. Alors les facteurs $\mathfrak{L}_1, \ldots, \mathfrak{L}_{l-2}$ ne peuvent tous avoir dans ce nombre M'' des exposants divisibles par l.

Car autrement on pourrait poser, d'après le théorème 153, $\mathsf{M}''=\Theta'\alpha'$, Θ' étant une unité de C et α' un entier de $c(\zeta)$. En considérant alors les égalités $\mathsf{M}^{1-S}=\zeta^{r-1}$, $\Lambda^{1-S}=\mathsf{E}$, $\Lambda'^{1-S}=\mathsf{E}'$ on aurait,

$$\Theta'^{1-S}=\mathsf{E}'\mathsf{E}^{r'}\zeta^{(rr'+r'')},$$

d'où on déduirait, à cause de (134),

$$(135)\qquad \Theta'^{1-S}=\mathsf{H}_1^{e'_1+r'e_1}\cdots\mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}+r'e_{\frac{l-3}{2}}}\mathsf{H}_{\frac{l-1}{2}}^{r'e_{\frac{l-1}{2}}}\varepsilon,$$

ε étant une unité de $c(\zeta)$; mais cette relation est incompatible avec la définition des unités fondamentales relatives (§ 55); car chacun des nombres $e_{\frac{l-1}{2}}$, $e'_{\frac{l-1}{2}}$ étant premier à l, les exposants de $\mathsf{H}_{\frac{l-3}{2}}$, $\mathsf{H}_{\frac{l-1}{2}}$ dans (135) ne sont certainement pas tous deux divisibles par l. Si donc, par exemple, $\mathfrak{L}_{t-2}$ figure dans M'' avec un exposant non divisible par l, on en conclut que la classe L_{t-2} est un produit de puissances des classes $L_1, \ldots, L_{t-3}$ et d'une classe contenant des idéaux de $c(\zeta)$.

Les mêmes considérations que dans le cas de $m=\frac{l-3}{2}$ montrent encore, dans le cas actuel de $m=\frac{l-5}{2}$, que les classes d'idéaux $L_1, \ldots, L_{t-3}$ ne peuvent former aucune classe

$$k'''=L_1^{a'''_1}\cdots L_{t-3}^{a'''_{t-3}}$$

contenant des idéaux de $c(\zeta)$, si les exposants a''' sont des entiers rationnels non tous divisibles par l. $L_1, \ldots, L_{t-3}$ forment donc une base de la famille de classes composée de tous les idéaux invariants; son degré est par suite $t-3$, ce qui est conforme au théorème 158.

En continuant par le même procédé, on arrive à démontrer complètement le théorème 158.

Nous avions exclu le cas où le corps kummerien C serait défini par un nombre $\sqrt[l]{\varepsilon}$, ε étant une unité de $c(\zeta)$; il nous reste donc à traiter ce cas à part.

Le discriminant relatif du corps $C=c(\sqrt[l]{\varepsilon}, \zeta)$ ne peut alors, d'après le théorème 148, contenir d'autre facteur premier que $\mathfrak{l}$. On a dans C la décomposition $\mathfrak{l}=\mathfrak{L}^l$ et $\mathfrak{L}$ est le seul idéal premier invariant de C. Soient encore $\eta_1, \ldots, \eta_{\frac{l-1}{2}}$, les normes relatives des $\frac{l-1}{2}$ unités fondamentales relatives $\mathsf{H}_1, \ldots, \mathsf{H}_{\frac{l-1}{2}}$. Comme le degré d'une famille d'unités de $c(\zeta)$ est toujours $\leqslant\frac{l-1}{2}$, on a certainement une relation de la forme

$$(136)\qquad \eta_1^{e_1}\cdots\eta_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}}\varepsilon^{e_{\frac{l+1}{2}}}=\eta^{l},$$

où $e_1, \ldots, e_{\frac{l-1}{2}}, e_{\frac{l+1}{2}}$ sont des entiers rationnels non tous divisibles par l et η une unité de $c(\zeta)$. En posant

(137) $$\mathsf{H} = \mathsf{H}_1^{e_1} \cdots \mathsf{H}_{\frac{l-1}{2}}^{e_{\frac{l-1}{2}}} (\sqrt[l]{\varepsilon})^{e_{\frac{l+1}{2}}} \eta^{-1},$$

on a $\mathrm{N}_s(\mathsf{H}) = 1$, et par suite (théorème 90) $\mathsf{H} = \mathsf{\Lambda}^{1-S}$, $\mathsf{\Lambda}$ étant un entier de C; on peut alors poser(¹) $\mathsf{\Lambda} = \mathfrak{L}^a \mathfrak{j}$, $\mathfrak{j}$ étant un idéal de $c(\zeta)$. L'exposant a n'est pas divisible par l, car autrement, comme $\mathfrak{L}^l = \mathfrak{l} = 1 - \zeta$, on aurait, vu le théorème 153, $\mathsf{\Lambda} = \Theta\alpha$, Θ étant une unité de C et α un nombre de $c(\zeta)$; mais on aurait alors $\mathsf{H} = \Theta^{1-S}$, et par suite, à cause de (137), une contradiction avec la définition des unités fondamentales relatives (§ 55). De l'égalité $\mathsf{\Lambda} = \mathfrak{L}^a \mathfrak{j}$, nous tirons $\mathfrak{j}^l \sim 1$; donc $\mathfrak{j} \sim 1$, $\mathfrak{L}^a \sim 1$, et comme a est premier à l, $\mathfrak{L} \sim 1$, c'est-à-dire que le seul idéal invariant du cas actuel est un idéal principal. Le degré de la famille de classes de tous les idéaux invariants est par suite égal à o dans le cas actuel.

Supposons maintenant que parmi les exposants $e_1, \ldots, e_{\frac{l+1}{2}}$, $e_{\frac{l+1}{2}}$, par exemple, soit premier à l et démontrons qu'il ne peut exister aucune relation

(138) $$\eta_1^{e'_1} \cdots \eta_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} \varepsilon^{e'_{\frac{l-1}{2}}} = \eta'^l,$$

où $e'_1, \ldots, e'_{\frac{l-3}{2}}, e'_{\frac{l-1}{2}}$ soient des entiers rationnels non tous divisibles par l et η' une unité de $c(\zeta)$. En effet, on en déduirait que

$$\mathsf{H}' = \mathsf{H}_1^{e'_1} \cdots \mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}} (\sqrt[l]{\varepsilon})^{e'_{\frac{l-1}{2}}} \eta'^{-1}$$

est une unité de norme relative égale à 1. Posons, d'après le théorème 90, $\mathsf{H}' = \mathsf{\Lambda}'^{1-S}$, $\mathsf{\Lambda}'$ étant un entier de C, et déterminons un exposant entier positif r tel que $\mathfrak{L}$ ait dans $\mathsf{\Lambda}'\mathsf{\Lambda}^r$ un exposant divisible par l. On peut alors, vu le théorème 153, poser $\mathsf{\Lambda}'\mathsf{\Lambda}^r = \Theta'\alpha'$, Θ' étant une unité de C et α' un entier de $c(\zeta)$; alors on a $\Theta'^{1-S} = \mathsf{H}'\mathsf{H}^r$, c'est-à-dire que l'unité

$$\mathsf{H}_1^{e'_1+re_1} \cdots \mathsf{H}_{\frac{l-3}{2}}^{e'_{\frac{l-3}{2}}+re_{\frac{l-3}{2}}} \mathsf{H}_{\frac{l-1}{2}}^{re_{\frac{l-1}{2}}} (\sqrt[l]{\varepsilon})^{e'_{\frac{l-1}{2}}+re_{\frac{l+1}{2}}} \eta'^{-1}\eta^{-r}$$

serait la $(1 - S)^{\text{ième}}$ puissance symbolique d'une unité de C, ce qui est incompatible avec la définition des unités fondamentales relatives. Une relation telle que (138) est donc impossible; vu (136), et comme $e_{\frac{l+1}{2}}$ est premier à l, $\eta_1, \ldots, \eta_{\frac{l-1}{2}}, \varepsilon$ forment donc une base de la famille d'unités formée des normes relatives de toutes les unités

(¹) N. T. — Parce que $\mathfrak{L}$ est le seul idéal invariant de C.

de C. Le degré de cette famille est donc $\frac{l-1}{2}$ et, par suite, toute unité de $c(\zeta)$ est la norme relative d'une unité de C. On a donc

$$l + m - \frac{l+1}{2} = 0,$$

et le théorème 158 est encore établi dans ce cas.

§ 148. — La totalité des classes d'idéaux invariantes.

Le théorème 158 a mis en lumière une relation remarquable qui existe entre la famille de classes formée de tous les idéaux invariants et la famille d'unités formée par les normes relatives de toutes les unités de C. Il y a une relation aussi importante entre la famille de classes formée de toutes les classes invariantes et une certaine famille d'unités de $c(\zeta)$.

Théorème 159. — *Soit t le nombre des idéaux premiers qui divisent le discriminant relatif du corps kummerien régulier C de degré relatif l; toutes les unités de $c(\zeta)$ égales à la norme relative soit d'une unité de C, soit d'une fraction de C, forment une famille d'unités : si n est son degré, la famille de classes formée de toutes les classes invariantes est de degré $t + n - \frac{l+1}{2}$.*

Démonstration. — Donnons à m le même sens que dans le théorème 158. Si, *en premier lieu, $n = m$*, la famille d'unités en question coïncide avec celle du théorème 158, c'est-à-dire qu'une unité de $c(\zeta)$ égale à la norme relative d'une fraction de C est en même temps toujours égale à la norme relative d'une unité de C. Démontrons alors que, dans ce cas, la famille de classes des idéaux invariants est la famille de toutes les classes invariantes. En effet, A étant une classe invariante de C et $\mathfrak{A}$ un idéal de A, nous pouvons poser $\mathfrak{A}^{1-S} = \mathfrak{a}$, $\mathfrak{a}$ étant un certain nombre entier ou fractionnaire de C, et la norme relative $N_{\zeta}(\mathfrak{a})$ est alors évidemment égale à une unité ε de $c(\zeta)$. Comme ensuite, dans le cas actuel, $n = m$, on peut aussi trouver dans C une unité H telle que $N_{\zeta}(\mathsf{H}) = \varepsilon$, on a $N_{\zeta}(\mathfrak{a}^{-1}\mathsf{H}) = 1$, et par suite (théorème 90) $\mathfrak{a}^{-1}\mathsf{H} = \mathfrak{b}^{1-S}$ ou $\mathfrak{a}\mathfrak{b}^{1-S} = \mathsf{H}$, $\mathfrak{b}$ étant un nombre convenable de C. A cause de $\mathfrak{a} = \mathfrak{A}^{1-S}$, on a $(\mathfrak{A}\mathfrak{b})^{1-S} = \mathsf{H}$, c'est-à-dire que $\mathfrak{A}\mathfrak{b}$ est le produit d'un idéal invariant et d'un idéal de $c(\zeta)$, et par suite on obtient la classe A en multipliant une classe contenant un idéal invariant par une classe contenant des idéaux de $c(\zeta)$. Notre assertion est donc justifiée et le degré de la famille de classes formée de toutes les classes invariantes est alors (vu le théorème 158) égal à $t + m - \frac{l+1}{2}$, ce qui est conforme au théorème 159, si $n = m$.

Soit, *en second lieu*, $n = m + 1$; il existe alors dans $c(\zeta)$ une unité ε, qui n'est pas égale à la norme relative d'une unité de C, mais est la norme relative d'une fraction $\mathfrak{a}$ de C, et toute autre unité ε' de même nature sera égale à $\varepsilon' = \varepsilon^a \eta$, a étant un exposant entier et η la norme relative d'une unité de C. Posons

$$\mathfrak{a} = \mathfrak{P}_1^{G_1(S)} \dots \mathfrak{P}_r^{G_r(S)},$$

$\mathfrak{P}_1, \dots, \mathfrak{P}_r$ étant des idéaux premiers distincts de C, dont aucun n'est conjugué relatif d'un autre et où $G_1(S), \dots, G_r(S)$ sont des polynômes à coefficients entiers de degré $l - 1$ en S. Comme $N_c(\mathfrak{a}) = \varepsilon$, on a

$$\left(\mathfrak{P}_1^{G_1(S)} \dots \mathfrak{P}_r^{G_r(S)}\right)^{1+S+\dots+S^{l-1}} = \varepsilon,$$

d'où l'on déduit aisément que tous les polynômes G sont divisibles par $1 - S$. Posons

$$G_1(S) = (1 - S)G_1(S), \quad \dots, \quad G_r(S) = (1 - S)G_r(S)$$

et

$$\mathfrak{P}_1^{G_1(S)} \dots \mathfrak{P}_r^{G_r(S)} = \mathfrak{A}\alpha,$$

$\mathfrak{A}$ étant un idéal de C et α un entier ou une fraction de $c(\zeta)$; on a, dès lors, $\mathfrak{a} = \mathfrak{A}^{1-S}$. Il en résulte d'abord que $\mathfrak{A}$ détermine une classe invariante. Cette classe invariante A ne contient pas d'idéal égal au produit d'un idéal invariant par un idéal de $c(\zeta)$; en effet, on pourrait dans ce cas poser $\mathfrak{A} = \mathfrak{c}\mathfrak{L}\mathfrak{j}$, $\mathfrak{c}$ étant un entier ou une fraction de C, $\mathfrak{L}$ un idéal invariant de C et $\mathfrak{j}$ un idéal de $c(\zeta)$; on aurait alors $\mathfrak{A}^{1-S} = \mathfrak{c}^{1-S}$, c'est-à-dire $\mathfrak{a} = \mathsf{H}\mathfrak{c}^{1-S}$, H étant une unité de C. Il en résulterait $N_c(\mathfrak{a}) = N_c(\mathsf{H}) = \varepsilon$, contrairement à l'hypothèse sur ε.

Nous allons montrer maintenant que, dans le cas actuel $n = m + 1$, toute classe invariante donnée A' est de la forme $A' = A^a L k$, où A^a est une puissance de la classe A qui vient d'être déterminée, L une classe avec un idéal invariant et k une classe contenant des idéaux de $c(\zeta)$. Pour cela, prenons dans A' un idéal quelconque $\mathfrak{A}'$; nous pouvons poser ensuite $\mathfrak{A}'^{1-S} = \mathfrak{a}'$, $\mathfrak{a}'$ étant un nombre convenable de C. Alors $N_c(\mathfrak{a}') = \varepsilon'$ est une unité de $c(\zeta)$; posons, conformément à notre hypothèse, $N_c(\mathfrak{a}') = \varepsilon^a \eta$, ε, a, η ayant le sens de tout à l'heure. Soit $\mathfrak{a}$ le nombre déjà considéré pour lequel $\varepsilon = N_c(\mathfrak{a})$; soit, de plus, $\eta = N_c(\mathsf{H})$, H étant une unité de C. On tire de cette équation $N_c(\mathfrak{a}'^{-1}\mathfrak{a}^a\mathsf{H}) = 1$, et alors (théorème 90) $\mathfrak{a}'^{-1}\mathfrak{a}^a\mathsf{H} = \mathfrak{c}^{1-S}$, $\mathfrak{c}$ étant un nombre convenable de C, on en tire $(\mathfrak{A}'^{-1}\mathfrak{A}^a\mathfrak{c}^{-1})^{1-S} = 1$. Cette égalité montre que $\mathfrak{A}'^{-1}\mathfrak{A}^a\mathfrak{c}^{-1}$ devient, après multiplication par un entier convenable de $c(\zeta)$, le produit d'un idéal invariant $\mathfrak{L}$ par un idéal $\mathfrak{j}$ de $c(\zeta)$; on a donc $\mathfrak{A}' \sim \mathfrak{A}^a\mathfrak{L}\mathfrak{j}$. Par conséquent, à cause de $n = m + 1$, le degré de la famille de toutes les classes invariantes est $l + m + 1 - \frac{l+1}{2}$, valeur conforme au théorème 159.

Soit, *en troisième lieu*, $n = m + 2$; il existe alors dans $c(\zeta)$, outre ε, encore une unité ε' égale à la norme relative d'une fraction $\mathfrak{a}'$ de C, et cependant elle ne peut se mettre sous la forme $\varepsilon' = \varepsilon^a \eta$, η étant la norme relative d'une unité de C. Posons

$$\mathfrak{a}' = \mathfrak{P}_1'^{G_1'(S)} \ldots \mathfrak{P}_r'^{G_r'(S)}$$

(les $\mathfrak{P}'$ et les G' satisfaisant aux mêmes conditions que les $\mathfrak{P}$ et les G plus haut) Comme $N_c(\mathfrak{a}') = \varepsilon'$, on a

$$\left(\mathfrak{P}_1'^{G_1'(S)} \ldots \mathfrak{P}_r'^{G_r'(S)}\right)^{1+S+\ldots+S^{l-1}} = \varepsilon',$$

les G' doivent alors être divisibles par $1 - S$. Posons

$$G_1'(S) = (1 - S)G_1''(S), \quad \ldots, \quad G_r'(S) = (1 - S)G_r''(S)$$

et

$$\mathfrak{P}_1'^{G_1''(S)} \ldots \mathfrak{P}_r'^{G_r''(S)} = \mathfrak{A}'\alpha'.$$

$\mathfrak{A}'$ étant un idéal de C et α' un nombre de $c(\zeta)$, on a $\mathfrak{a}' = \mathfrak{A}'^{1-S}$. L'idéal $\mathfrak{A}'$ définit donc une classe invariante A′. Cette classe ne peut se représenter par $A' = A^a Lk$, A^a étant une puissance de la classe A, L une classe à idéal invariant et k une classe contenant des idéaux de $c(\zeta)$. En effet, il en résulterait, pour $\mathfrak{A}'$, $\mathfrak{A}' = \mathfrak{c}\mathfrak{A}^a L\mathfrak{j}$, $\mathfrak{c}$ étant un nombre de C, L un idéal invariant et $\mathfrak{j}$ un idéal de $c(\zeta)$; mais alors on aurait $\mathfrak{A}'^{1-S} = \mathfrak{c}^{1-S}\mathfrak{A}^{a(1-S)} = \mathfrak{c}^{1-S}\mathfrak{a}^a$, c'est-à-dire $\mathfrak{a}' = H\mathfrak{c}^{1-S}\mathfrak{a}^a$, H étant une unité de C. En prenant la norme relative, on aurait $N_c(\mathfrak{a}') = \varepsilon' = \varepsilon^a N_c(H)$, ce qui est impossible.

Dans le cas actuel $n = m + 2$, toute unité ε'' de $c(\zeta)$ égale à la norme relative d'un nombre de C est de la forme $\varepsilon'' = \varepsilon'^{a'} \varepsilon^a \eta$, a', a étant des exposants entiers et η la norme relative d'une unité de C. Alors, par les mêmes considérations que plus haut, on montre que toute classe invariante A″ peut se représenter par $A'^{a'} A^a Lk$, A′, A étant les classes précédemment définies, L une classe à idéal invariant, k une classe contenant des idéaux de $c(\zeta)$. Le degré de la famille de classes formée de toutes les classes invariantes est alors $t + m + 2 - \frac{l+1}{2}$, ce qui est la formule du théorème 159 pour $n = m + 2$.

En continuant ainsi, on démontre complètement le théorème 159.

§ 149. — Caractères d'un nombre et d'un idéal dans un corps kummerien régulier.

Il s'agit maintenant d'étudier la répartition des classes d'idéaux d'un corps kummerien régulier $C = c(\sqrt[l]{\mu}, \zeta)$, au même point de vue que la répartition en genres des classes d'un corps quadratique. Nous désignons par $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ les t idéaux pre-

miers distincts de $c(\zeta)$ qui divisent le discriminant relatif de C. A tout nombre entier $\nu(\neq 0)$ de $c(\zeta)$ répondent des valeurs déterminées des t symboles :

$$(139) \qquad \left\{\frac{\nu,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\nu,\ \mu}{\mathfrak{l}_t}\right\};$$

ces symboles représentent (§ 131) des racines $l^{\text{ièmes}}$ de l'unité. Ces t racines de l'unité (139) s'appellent *les caractères du nombre* ν dans le corps kummerien C. Pour un idéal $\mathfrak{J}$ du corps kummerien, prenons la norme relative $N_c(\mathfrak{J}) = \mathfrak{j}$. Soit h le nombre de classes de $c(\zeta)$ et h^* un entier positif, tel que l'on ait $hh^* \equiv 1$, mod l. Alors $\mathfrak{j}^{hh^*}$ est un idéal principal de $c(\zeta)$. Soit $\mathfrak{j}^{hh^*} = (\nu)$, ν étant un entier de $c(\zeta)$. Soit encore ξ_1 une unité de $c(\zeta)$. Alors si pour toute unité ξ_1 les t symboles

$$\left\{\frac{\xi_1,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\xi_1,\ \mu}{\mathfrak{l}_t}\right\}$$

ont la valeur 1, nous poserons $r = t$ et nous appellerons les r racines de l'unité

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\nu,\ \mu}{\mathfrak{l}_t}\right\}$$

les caractères de l'idéal $\mathfrak{J}$; ils sont parfaitement définis par cet idéal.

S'il existe, d'autre part, une unité ε_1 dans $c(\zeta)$, telle que l'un au moins des t symboles

$$\left\{\frac{\varepsilon_1,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\varepsilon_1,\ \mu}{\mathfrak{l}_t}\right\}$$

soit différent de 1, nous pouvons, sans diminuer la généralité, supposer que, par exemple, $\left\{\frac{\varepsilon,\ \mu}{\mathfrak{l}_t}\right\} = \zeta$.

Considérons alors toutes les unités ξ_2 de $c(\zeta)$ pour lesquelles $\left\{\frac{\xi_2,\ \mu}{\mathfrak{l}_t}\right\} = 1$. Soit, parmi elles, ε_2 une unité pour laquelle l'un au moins des symboles

$$\left\{\frac{\varepsilon_2,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\varepsilon_2,\ \mu}{\mathfrak{l}_{t-1}}\right\}$$

soit différent de 1 ; nous pouvons admettre que, par exemple, $\left\{\frac{\varepsilon_2,\ \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta$. Considérons toutes les unités ξ_3 pour lesquelles les deux derniers caractères relatifs à $\mathfrak{l}_t$ et $\mathfrak{l}_{t-1}$ sont égaux à 1, et voyons si elles en comprennent une ε_3, pour laquelle l'un au moins des $t-2$ symboles

$$\left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\varepsilon_3,\ \mu}{\mathfrak{l}_{t-2}}\right\}$$

soit $\neq 1$. En continuant ainsi, nous obtenons finalement un certain nombre r^*

d'unités $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{r^*}$ de $c(\zeta)$, telles que l'on a, en rangeant convenablement les idéaux $\mathfrak{l}_1, \ldots \mathfrak{l}_t$,

$$(140)\quad \left\{\begin{array}{l} \left\{\dfrac{\varepsilon_1, \mu}{\mathfrak{l}_t}\right\} = \zeta, \\[2ex] \left\{\dfrac{\varepsilon_2, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\dfrac{\varepsilon_2, \mu}{\mathfrak{l}_{t-1}}\right\} = \zeta, \\[2ex] \ldots\ldots\ldots\ldots\ldots \\[2ex] \left\{\dfrac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \left\{\dfrac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_{t-1}}\right\} = 1, \quad \ldots, \quad \left\{\dfrac{\varepsilon_{r^*}, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = \zeta, \end{array}\right.$$

et que de plus, pour toute unité ξ qui vérifie les r^* conditions,

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \ldots, \quad \left\{\frac{\xi, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = 1,$$

les $r = t - r^*$ caractères

$$\left\{\frac{\xi, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \left\{\frac{\xi, \mu}{\mathfrak{l}_r}\right\}$$

sont aussi tous égaux à 1.

Multiplions alors le nombre ν de $c(\zeta)$ déduit plus haut de l'idéal $\mathfrak{J}$ par des puissances des unités $\varepsilon_1, \ldots, \varepsilon_{r^*}$, de façon que le produit obtenu $\bar{\nu}$ vérifie les conditions

$$\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_t}\right\} = 1, \quad \ldots, \quad \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{t-r^*+1}}\right\} = 1;$$

j'appelle alors les $r = t - r^*$ unités :

$$\chi_1(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \chi_r(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_r}\right\},$$

les *caractères de l'idéal* $\mathfrak{J}$. Dans le paragraphe 151, nous verrons que l'on a toujours $r^* < t$ et, par suite, $r \geqq 1$.

§ 150. — Caractères d'une classe et notion de genre.

Le théorème 151 et les remarques additionnelles, paragraphe 133, conduisent à la proposition :

Théorème 160. — Les idéaux d'une seule et même classe d'un corps kummerien régulier ont tous les mêmes caractères

Il est ainsi possible de faire correspondre à toute classe d'idéaux un système déterminé de caractères. Nous rangerons, comme au paragraphe 66 pour le corps quadratique, toutes les classes ayant les mêmes caractères, dans un *genre*, et nous

appellerons en particulier *genre principal* celui dont tous les caractères sont égaux à 1. Comme c'est le cas de la classe principale, celle-ci appartient donc toujours au genre principal. Les premières formules (80) et (83) conduisent facilement aux propositions suivantes : G et G' étant deux genres quelconques, si l'on multiplie chaque classe de G par chaque classe de G', les produits forment encore un genre : on l'appellera *le produit des genres* G et G'. Les caractères en seront les produits des caractères correspondants de G et G'.

De la définition résulte que les classes conjuguées relatives SK, ..., S^{l-1}K d'une classe K font partie du même genre que K, et, par suite, la $(1 + S)^{\text{ième}}$ puissance symbolique d'une classe K quelconque appartient au genre principal. Enfin, il est évident que tous les genres d'un corps kummerien contiennent le même nombre de classes.

§ 151. — Limites supérieures du degré de la famille issue de toutes les classes invariantes.

Comme pour le corps quadratique, se pose la question importante de savoir si un système arbitraire de r racines $l^{\text{ièmes}}$ de l'unité peut former les caractères d'un genre du corps kummerien. Cette question ne sera complètement éclaircie qu'au chapitre XXXIV. Dans ce paragraphe et le suivant nous placerons seulement quelques lemmes nécessaires pour la suite.

Lemme 33. — t et n ayant le même sens qu'au théorème 159 et r étant le nombre des caractères distinctifs du genre d'une classe, on a toujours

$$t + n - \frac{l+1}{2} \leqq r - 1.$$

Démonstration. — Soient $\varepsilon_1, \dots, \varepsilon_{r^*}$, les r^* unités particulières de $c(\zeta)$ introduites paragraphe 149. Alors on a $r = t + r^*$. Soient $\eta_1, \dots, \eta_n$ une base de la famille d'unités de $c(\zeta)$, normes relatives de nombres de C. Supposons qu'il existe entre les $r^* + n$ unités $\varepsilon_1, \dots, \varepsilon_{r^*}, \eta_1, \dots, \eta_n$ une relation

$$(141) \qquad \varepsilon_1^{a_1} \dots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \dots \eta_n^{b_n} = \varepsilon^l,$$

les exposants $a_1, \dots, a_{r^*}, b_1, \dots, b_n$ étant des entiers rationnels non tous divisibles par l et ε étant une unité convenable de $c(\zeta)$; on devrait alors toujours avoir pour $u = 1, 2, \dots, t$

$$\left\{\frac{\varepsilon_1^{a_1} \dots \varepsilon_{r^*}^{a_{r^*}} \eta_1^{b_1} \dots \eta_n^{b_n}, \mu}{\mathfrak{l}_u}\right\} = 1,$$

et si l'on remarque que les unités η sont normes relatives de nombres de C et que,

par suite, on a toujours $\left\{\frac{\eta_v, \mu}{\mathfrak{l}_u}\right\} = 1$ pour $u = 1, 2, \ldots, l$ et $v = 1, 2, \ldots, n$, on aurait aussi

$$\left\{\frac{\varepsilon_1^{a_1} \ldots \varepsilon_r^{a_r}, \mu}{\mathfrak{l}_u}\right\} = 1.$$

Ceci n'est possible, vu les formules (140) pour les unités $\varepsilon_1, \ldots, \varepsilon_r$, que si les exposants $a_1, \ldots, a_{r^*}$ sont divisibles par l, et la relation (141) prendrait alors la forme

$$\eta_1^{b_1} \ldots \eta_n^{b_n} = \varepsilon^{*l},$$

ε^* étant encore une unité de $c(\zeta)$. Mais comme les η forment une base d'une famille d'unités de $c(\zeta)$, une telle relation n'est possible que si tous les b sont divisibles par l. Il résulte de là que la relation supposée (141) ne peut exister, c'est-à-dire que les unités $\varepsilon_1, \ldots, \varepsilon_{r^*}, \eta_1, \ldots, \eta_n$ forment une base de famille d'unités; le degré de cette famille est $r^* + n$, et comme le degré d'une famille d'unités est au plus $\frac{l-1}{2}$, on a $r^* + n \leqq \frac{l-1}{2}$, ce qu'il fallait démontrer. Comme on a $l + n - \frac{l+1}{2} = 0$, il en résulte qu'on a toujours $r < l$, donc $r \geqq 1$.

§ 152. — Complexes d'un corps kummerien-régulier.

Soit h le nombre des classes d'idéaux du corps circulaire régulier $c(\zeta)$; il existe alors dans le corps kummerien $C = c(\sqrt[l]{\mu}, \zeta)$ exactement h classes d'idéaux distinctes, contenant des idéaux de $c(\zeta)$. En effet, toute classe de $c(\zeta)$ donne évidemment une classe de K de cette espèce, et si deux classes distinctes k_1, k_2 de $c(\zeta)$ contenaient des idéaux équivalents dans C, un idéal $\mathfrak{j}$ de $c(\zeta)$ dans la classe $\frac{k_1}{k_2}$ devrait toujours devenir principal dans C. Mais alors, d'après le théorème 153, $\mathfrak{j}$ serait aussi principal dans $c(\zeta)$, contrairement à l'hypothèse $k_1 \neq k_2$.

K étant alors une classe quelconque de C et $k_1, \ldots, k_h$ les h classes de C contenant des idéaux de $c(\zeta)$, j'appellerai l'ensemble des h classes $k_1 K, \ldots, k_h K$ un *complexe*. Le complexe $k_1, \ldots, k_h$ sera le *complexe principal* et se représentera par 1. Les h classes d'un complexe quelconque P font évidemment partie du même genre; ce genre s'appellera le *genre du complexe* P.

Si une classe d'un complexe P est invariante, il en est de même des autres; le complexe sera dit *invariant*.

P et P′ étant deux complexes quelconques, les produits d'une classe quelconque de l'un par une classe quelconque de l'autre forment encore un complexe : ce sera le *produit* PP′ *des complexes* P *et* P′.

K étant une classe du complexe P, le complexe auquel appartient SK sera SP; j'appellerai le complexe Q, dont le produit par SP donne le complexe P, *la* $(1-S)^{\text{ième}}$ *puissance symbolique du complexe* P, $Q = P^{1-S}$.

Si $P^{1-S} = 1$ (complexe principal), P est un complexe invariant. En effet, K étant une classe de P, $P^{1-S} = 1$ entraîne évidemment $K^{1-S} = k$, k étant une des classes $k_1, \ldots, k_h$. En prenant la norme relative, on obtient $1 = k^l$, et comme d'ailleurs $k^h = 1$, il en résulte $k = 1$, c'est-à-dire $K^{1-S} = 1$: K est une classe invariante et P un complexe invariant.

§ 153. — Limites supérieures du nombre des genres d'un corps kummerien régulier.

Lemme 34. — l et n ayant le sens du théorème 159, g étant le nombre des genres du corps kummerien régulier C, on a toujours

$$g \leqq l^{l+n-\frac{l+1}{2}}.$$

Démonstration. — g étant le nombre des genres du corps kummerien, les complexes se répartissent aussi en g genres. Si l'on désigne par f le nombre des complexes du genre principal, on a donc pour le nombre total M des complexes, $M = fg$.

Cherchons maintenant le nombre a des complexes invariants. Pour cela, observons que, d'après le théorème 159, le degré de la famille issue de toutes les classes invariantes est égal à $l + n - \frac{l+1}{2}$. Soit $A_1, \ldots, A_{l+n-\frac{l+1}{2}}$ une base de cette famille: l'expression

$$A_1^{u_1} \ldots A_{l+n-\frac{l+1}{2}}^{u_{l+n-\frac{l+1}{2}}}$$

représente alors, lorsque les exposants prennent séparément toutes les valeurs 0, 1, ..., $l-1$, des classes toutes invariantes, faisant partie de complexes distincts, et par suite ces classes forment $l^{l+n-\frac{l+1}{2}}$ complexes. Toute classe invariante A est de la forme

$$A = A_1^{a_1} \ldots A_{l+n-\frac{l+1}{2}}^{a_{l+n-\frac{l+1}{2}}} k,$$

les a étant des entiers rationnels et k une classe de $c(\zeta)$. En nous rappelant alors que les $l^{\text{ièmes}}$ puissances des classes invariantes $A_1, \ldots, A_{l+n-\frac{l+1}{2}}$ sont des classes contenant des idéaux de $c(\zeta)$, il en résulte que A appartient nécessairement à l'un des $l^{l+n-\frac{l+1}{2}}$ complexes précédemment déterminés; le nombre cherché $a = l^{l+n-\frac{l+1}{2}}$.

Les définitions des paragraphes 150 et 152 montrent de suite que la $(1-S)^{\text{ième}}$ puissance symbolique d'un complexe quelconque est un complexe du genre principal.

Envisageons les complexes du genre principal qui sont des $(1-S)^{\text{ièmes}}$ puissances symboliques de complexes; soit f' leur nombre et soient $P_1 = G_1^{1-S}, \ldots, P_{f'} = G_{f'}^{1-S}$ ces complexes. P étant alors un complexe quelconque, P^{1-S} est nécessairement l'un des f' complexes $P_1, \ldots, P_{f'}$; soit $P^{1-S} = P_r$. Alors on a $P^{1-S} = G_r^{1-S}$, c'est-à-dire $(PG_r^{-1})^{1-S} = 1$, et par suite PG_r^{-1} est un complexe invariant A; on a $P = AG_r$, et par suite l'expression AG_r embrasse tous les complexes, si l'on prend pour A tous les complexes invariants et pour G_r les f' complexes $G_1, \ldots, G_{f'}$. Il est aussi évident que cette représentation est unique; le nombre de tous les complexes est donc $M = af'$. On a donc $af' = gf$, et comme on a $f' \leqq f$, il en résulte $g \leqq a$, c'est-à-dire

$$g \leqq l^{t+m-\frac{l+1}{2}},$$

ce qui démontre le lemme 34.

Lemme 35. — Les lemmes 33 et 34 conduisent de suite au suivant; r étant le nombre des caractères distinctifs du genre d'une classe, le nombre des genres g est $\leqq l^{r-1}$.

CHAPITRE XXXIII.

Loi de réciprocité des résidus de $l^{\text{ièmes}}$ puissances dans un corps circulaire régulier.

§ 154. — La loi de réciprocité des résidus de $l^{\text{ièmes}}$ puissances et les lois complémentaires.

Les théories développées jusqu'ici nous permettent de démontrer certaines lois fondamentales sur les résidus de puissances $l^{\text{ièmes}}$ dans un corps circulaire régulier; elles correspondent aux lois de réciprocité des restes quadratiques dans le domaine des nombres rationnels, et la loi de réciprocité d'Eisenstein (théorème 140, § 115) entre un nombre quelconque de $c(\zeta)$ et un nombre rationnel en est un cas particulier. Pour donner à ces lois leur expression la plus simple, généralisons le symbole $\left(\frac{\nu}{\mathfrak{w}}\right)$ défini aux paragraphes 113 et 127.

Soit h le nombre des classes d'idéaux de $c(\zeta)$; déterminons un entier positif h^* tel que l'on ait $hh^* \equiv 1$, mod l. $\mathfrak{p}$ désignant alors un idéal premier quelconque de $c(\zeta)$, différent de $\mathfrak{l}$, $\mathfrak{p}^{hh^*}$ est toujours un idéal principal de $c(\zeta)$; posons $\mathfrak{p}^{hh^*} = (\pi)$, π étant un entier de $c(\zeta)$, et supposons, ce qui est possible d'après le théorème 157, que π soit primaire. Un tel nombre π s'appellera un *nombre primaire de* $\mathfrak{p}$. Toute unité

primaire de $c(\zeta)$ étant la $l^{\text{ième}}$ puissance d'une unité de $c(\zeta)$ (remarque du § 142), π possède vis-à-vis de tout idéal premier autre que $\mathfrak{p}$ un caractère de puissance complètement déterminé. $\mathfrak{q}$ étant alors un idéal premier quelconque de $c(\zeta)$ autre que $\mathfrak{l}$ et $\mathfrak{p}$, on définira le *symbole* $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)$ par la formule

$$\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=\left(\frac{\pi}{\mathfrak{q}}\right).$$

Ce symbole est donc une racine $l^{\text{ième}}$ déterminée de l'unité, définie par les deux idéaux premiers $\mathfrak{p}$ et $\mathfrak{q}$. En utilisant ce symbole, nous énoncerons le théorème

THÉORÈME 161. — *$\mathfrak{p}$ et $\mathfrak{q}$ étant deux idéaux premiers distincts, autres que $\mathfrak{l}$, du corps circulaire régulier $c(\zeta)$, on a*

$$\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right),$$

relation appelée loi de réciprocité des restes de $l^{\text{ièmes}}$ puissances. De plus, si ε est une unité quelconque de $c(\zeta)$ et π un nombre primaire de $\mathfrak{p}$, on a

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right)=\left(\frac{\pi,\ \varepsilon}{\mathfrak{l}}\right),\qquad \left(\frac{\lambda}{\mathfrak{p}}\right)=\left(\frac{\pi,\ \lambda}{\mathfrak{l}}\right),$$

relations appelées lois complémentaires de la loi de réciprocité. [Kummer[10, 12, 18, 19, 20, 21].]

Nous démontrerons progressivement ce théorème fondamental dans les paragraphes suivants (§§ 155-161), en appliquant à des corps kummeriens réguliers particuliers les théorèmes et lemmes du précédent chapitre.

§ 155. — IDÉAUX PREMIERS DE PREMIÈRE ET DE SECONDE ESPÈCE DANS UN CORPS CIRCULAIRE RÉGULIER.

Il est nécessaire de distinguer pour la suite deux espèces d'idéaux premiers dans $c(\zeta)$; un idéal premier $\mathfrak{p}$ autre que $\mathfrak{l}$ de $c(\zeta)$ sera de *première espèce* lorsque toute unité de $c(\zeta)$ ne sera pas reste de $l^{\text{ième}}$ puissance mod $\mathfrak{p}$; dans le cas contraire, il sera de *seconde espèce*. [Kummer[20].]

LEMME 36. — *ε et η étant des unités quelconques du corps circulaire $c(\zeta)$, $\lambda = 1-\zeta$, $\mathfrak{l}=(\lambda)$, on a les égalités*

$$\left(\frac{\zeta,\ \varepsilon}{\mathfrak{l}}\right)=1,\qquad \left(\frac{\lambda,\ \varepsilon}{\mathfrak{l}}\right)=1.$$

Démonstration. — Si ε est la $l^{\text{ème}}$ puissance d'une unité de $c(\zeta)$, les formules ci-dessus sont évidentes. Dans le cas contraire, $\sqrt[l]{\varepsilon}$ définit un corps kummerien $c(\sqrt[l]{\varepsilon},\ \zeta)$,

et les considérations du paragraphe 147 s'appliquent à ce corps. Toutes les unités de $c(\zeta)$ et, de plus, le nombre λ, sont alors normes relatives de nombres de $c(\sqrt[l]{\varepsilon}, \zeta)$, d'où, vu le théorème 151, les égalités à démontrer.

Si l'on veut n'appliquer ici le théorème 151 pour $\mathfrak{w} = \mathfrak{l}$ que dans le cas traité en détail paragraphes 133, où $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, on achèvera en prenant d'abord, pour $\varepsilon = \zeta^{l-1}$; ensuite on aura $\left(\frac{\xi, \zeta}{\mathfrak{l}}\right) = 1$, $\left(\frac{\lambda, \zeta}{\mathfrak{l}}\right) = 1$ (¹). On déterminera ensuite, dans le cas de ε unité quelconque de $c(\zeta)$, une racine $l^{\text{ième}}$ de l'unité ζ^*, telle que l'on ait $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$, mod $\mathfrak{l}^2$. En prenant alors dans la démonstration précédente $\zeta^* \varepsilon^{l-1}$, au lieu de ε, on a, vu la deuxième formule (83), paragraphe 131,

$$\left(\frac{\xi, \varepsilon}{\mathfrak{l}}\right) = 1 \quad \text{et} \quad \left(\frac{\lambda, \varepsilon}{\mathfrak{l}}\right) = 1.$$

Lemme 37. — $\mathfrak{p}$ étant un idéal premier de première espèce et π un nombre primaire de $\mathfrak{p}$, il existe dans $c(\zeta)$ au moins une unité ε, pour laquelle on a

$$\left(\frac{\varepsilon, \pi}{\mathfrak{l}}\right) \neq 1.$$

Si, au contraire, $\mathfrak{q}$ est un idéal premier de seconde espèce et $\varkappa$ un nombre primaire de $\mathfrak{q}$, on a pour toute unité ξ de $c(\zeta)$

$$\left(\frac{\xi, \varkappa}{\mathfrak{l}}\right) = 1.$$

Démonstration. — Pour démontrer la première partie, supposons qu'on ait, au contraire, pour toute unité ξ de $c(\zeta)$,

$$\left(\frac{\xi, \pi}{\mathfrak{l}}\right) = 1.$$

Posons $\pi \equiv a + b\lambda^e$, mod $\mathfrak{l}^{e+1}$, a et b étant des entiers rationnels et e le plus grand exposant $\leqslant l-1$, pour lequel une telle relation est possible; π étant un nombre primaire, on doit avoir nécessairement $e > 1$ et $\pi . s^{\frac{l-1}{2}} \pi$ doit être congru mod l à un entier rationnel $\left(s^{\frac{l-1}{2}}\right.$ représente la substitution $(\zeta : \zeta^{-1})$ du corps circulaire $\left.c(\zeta)\right)$. Comme on a $s^{\frac{l-1}{2}} \lambda \equiv -\lambda$, mod $\mathfrak{l}^2$, on a

$$\pi . s^{\frac{l-1}{2}} \pi \equiv (a + b\lambda^e)(a + b(-\lambda)^e), \quad (\mathfrak{l}^{e+1}),$$

et il en résulte que, dans le cas de $e < l-1$, e doit être nécessairement impair.

(¹) N. T. — Voir la fin du § 131, et remarquer que $\zeta^{l-1} = (1-\lambda)^{l-1} \equiv 1 - (l-1)\lambda \equiv 1 + \lambda$, (mod $\mathfrak{l}^2$).

Nous avons trouvé, en démontrant le lemme 29, que les $l^* = \frac{l-3}{2}$ unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ du corps $c(\zeta)$ vérifiaient les conditions

$$\left.\begin{array}{l} l^{(u)}(\varepsilon_t) \equiv 0, \quad (l), \quad (u \neq 2t), \\ l^{(2t)}(\varepsilon_t) \not\equiv 0, \quad (l). \end{array}\right\} \qquad \begin{pmatrix} t = 1, 2, \ldots, l^* ; \\ u = 1, 2, \ldots, l-2. \end{pmatrix}$$

Si l'on porte, dans l'égalité $\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\} = 1$, successivement les unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ à la place de ξ, on déduit de la définition (82) du symbole $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ et de son extension (§ 131) les congruences

$$l^{(l-2)}(\pi^{l-1}) \equiv 0, \quad l^{(l-4)}(\pi^{l-1}) \equiv 0, \quad l^{(l-6)}(\pi^{l-1}) \equiv 0, \quad \ldots, \quad l^{(3)}(\pi^{l-1}) \equiv 0, \quad (\text{mod } l);$$

elles montrent que dans la congruence $\pi \equiv a + b\lambda^e$, mod $\mathfrak{l}^{e+1}$, e ne peut prendre aucune des valeurs $l-2$, $l-4$, $l-6$, ..., 3. Ceci joint aux conditions déjà trouvées pour e montre que $e = l-1$. Comme d'ailleurs $\lambda^{l-1} \equiv -l$, mod $\mathfrak{l}^l$, on a $\pi \equiv a - bl$, mod $\mathfrak{l}^l$, et, par suite, la norme de π vérifie la congruence

$$n(\pi) \equiv (a - bl)^{l-1} \equiv \pi^{l-1}, \quad (\mathfrak{l}^l).$$

D'autre part, on tire de la définition du symbole (§ 131) et du lemme 24 (§ 132)

$$\left\{\frac{\xi, \pi}{\mathfrak{l}}\right\} = \zeta^{\frac{1-n(\pi)}{l}},$$

et comme le symbole du premier membre doit être égal à 1, il en résulte $n(\pi) \equiv 1$, mod l^2, c'est-à-dire $\pi^{l-1} \equiv 1$, mod $\mathfrak{l}^l$, ou $\pi \equiv \pi^l$, mod $\mathfrak{l}^l$. D'après le théorème 148, le corps kummerien déterminé par $\sqrt[l]{\pi}$ possède, vu la dernière congruence, un discriminant relatif premier à $\mathfrak{l}$, et, par suite, $\mathfrak{p}$ est le seul idéal premier figurant dans le discriminant relatif de $c(\sqrt[l]{\pi}, \zeta)$.

Posons $\mathfrak{p} = \mathfrak{P}^l$; $\mathfrak{P}$ est le seul idéal invariant de ce corps. De $\sqrt[l]{\pi} = \mathfrak{P}^{hh^*} = \mathfrak{P}\mathfrak{p}^{\frac{hh^*-1}{l}}$ résulte que $\mathfrak{P}$ est équivalent à un idéal de $c(\zeta)$. La famille de tous les idéaux invariants est donc de degré 0 pour le corps kummerien $c(\sqrt[l]{\pi}, \zeta)$. Comme le nombre t des idéaux invariants de ce corps est 1, il résulte du théorème 158 : $1 + m - \frac{l+1}{2} = 0$, c'est-à-dire $m = \frac{l-1}{2}$. Par suite, toute unité de $c(\zeta)$ est norme relative d'une unité de $c(\sqrt[l]{\pi}, \zeta)$, et on a donc toujours (théorème 151) $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = 1$, et, par conséquent aussi, comme $\left\{\frac{\xi, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\xi^{hh^*}}{\mathfrak{p}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}^{hh^*}$, $\left\{\frac{\xi}{\mathfrak{p}}\right\} = 1$, contrairement à l'hypothèse que l'idéal $\mathfrak{p}$ est de première espèce.

Pour démontrer la seconde partie, considérons, comme dans le lemme 36, le corps kummerien $c(\sqrt[l]{\xi}, \zeta)$, ξ étant une unité quelconque de $c(\zeta)$, différente cepen-

dant de la $l^{ème}$ puissance d'une unité de $c(\zeta)$. Comme on l'a démontré à la fin du paragraphe 147, toute unité de $c(\zeta)$ est norme relative d'une unité de $c(\sqrt[l]{\xi}, \zeta)$ et les deux familles d'unités des théorèmes 158 et 159 ont, par suite, toutes deux le degré

$$m = n = \frac{l-1}{2}.$$

Comme, de plus, $t = 1$, le lemme 34 donne $g \leq 1$. Donc $g = 1$, toutes les classes d'idéaux du corps $c(\sqrt[l]{\xi}, \zeta)$ appartiennent au genre principal. $\mathfrak{q}$ étant idéal premier de deuxième espèce, on a $\left\{\frac{\xi}{\mathfrak{q}}\right\} = 1$, et, d'après le théorème 149, $\mathfrak{q}$ se décompose en l idéaux premiers distincts du corps $c(\sqrt[l]{\xi}, \zeta)$. Soit $\mathfrak{Q}$ l'un d'eux. Un nombre $\alpha (\neq 0)$ du corps $c(\zeta)$ a dans $c(\sqrt[l]{\xi}, \zeta)$ le caractère unique $\left\{\frac{\alpha, \xi}{\mathfrak{l}}\right\}$; ce dernier est toujours égal à 1 (lemme 36) si α est une unité de $c(\zeta)$. Le caractère de l'idéal premier $\mathfrak{Q}$ dans $c(\sqrt[l]{\xi}, \zeta)$ est, par suite, $\left\{\frac{\chi, \xi}{\mathfrak{l}}\right\}$, et ce dernier doit être égal à 1 d'après la proposition antérieure. Le lemme 37 est donc complètement démontré.

Si l'on voulait encore ne considérer le théorème 151 comme démontré dans le cas de $\mathfrak{w} = \mathfrak{l}$ que si $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, la répartition des genres, et en particulier le lemme 34, ne seraient aussi valables que dans ce cas. Nous devrions alors, pour démontrer la deuxième partie du lemme 37, prendre d'abord $\xi = \zeta^{l-1}$, puis $\xi = \zeta^* \varepsilon^{l-1}$, ε étant une unité quelconque de $c(\zeta)$ et ζ^* une racine $l^{ième}$ de l'unité, telle que l'on ait $\zeta^* \varepsilon^{l-1} \equiv 1 + \lambda$, mod $\mathfrak{l}^2$.

§ 156. — Lemmes sur les idéaux premiers de première espèce.

Lemme 38. — Soit $\mathfrak{p}$ un idéal premier de première espèce du corps circulaire régulier $c(\zeta)$ et π un nombre primaire de $\mathfrak{p}$. S'il existe alors dans $c(\zeta)$ une unité ε telle que l'on ait

$$\left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\} \neq 1, \quad \left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\},$$

on a pour toute unité ξ de $c(\zeta)$ l'égalité

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}.$$

Démonstration. — Le corps kummerien $c(\sqrt[l]{\pi}, \zeta)$ contient, $\mathfrak{p}$ étant un idéal premier de première espèce, deux idéaux premiers invariants $\mathfrak{L}$ et $\mathfrak{P}$, à savoir ceux dont les puissances $l^{ièmes}$ sont $\mathfrak{l}$ et $\mathfrak{p}$ (voir démonstration du lemme 37). L'idéal premier invariant $\mathfrak{P}$ étant évidemment idéal principal dans $c(\sqrt[l]{\pi}, \zeta)$, la famille de classes des

idéaux invariants de ce corps est de degré 0 ou 1, suivant que $\mathfrak{L}$ est ou non idéal principal. D'après le théorème 158, le nombre $2 + m - \frac{l+1}{2}$ est donc égal à 0 ou à 1, c'est-à-dire que l'on a $m = \frac{l-3}{2}$ ou $m = \frac{l-1}{2}$. Comme l'unité ε, vu l'hypothèse $\left\{\frac{\varepsilon, \pi}{\mathfrak{l}}\right\} \neq 1$, n'est certainement pas (théorème 151) norme relative d'une unité de $c(\sqrt[l]{\pi}, \zeta)$, on a nécessairement $m = \frac{l-3}{2}$, et, par suite, toute unité ξ de $c(\zeta)$ peut se mettre sous la forme $\xi = \varepsilon^a \eta$, a étant un entier rationnel et η une unité égale à la norme relative d'une unité de $c(\sqrt[l]{\pi}, \zeta)$. Pour ce motif, on a donc (théorème 151)

$$\left\{\frac{\eta, \pi}{\mathfrak{l}}\right\} = 1, \qquad \left\{\frac{\eta, \pi}{\mathfrak{p}}\right\} = \left\{\frac{\eta}{\mathfrak{p}}\right\} = 1,$$

et par suite aussi $\left\{\frac{\pi, \eta}{\mathfrak{l}}\right\} = \left\{\frac{\eta}{\mathfrak{p}}\right\}$; il en résulte, d'après la deuxième formule (83), que l'on a aussi $\left\{\frac{\pi, \xi}{\mathfrak{l}}\right\} = \left\{\frac{\xi}{\mathfrak{p}}\right\}$. C. q. f. d.

Si le théorème 151 n'est admis pour $\mathfrak{w} = \mathfrak{l}$ que si $\mu \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, on déterminera une racine $l^{\text{ième}}$ de l'unité ζ^*, telle que $\zeta^*\pi^{l-1} \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, et l'on considérera le corps $c(\sqrt[l]{\zeta^*\pi^{l-1}}, \zeta)$ au lieu de $c(\sqrt[l]{\pi}, \zeta)$. Puis on appliquera le lemme 36.

Lemme 39. — $\mathfrak{p}$, $\mathfrak{p}^*$ étant deux idéaux premiers de première espèce de $c(\zeta)$ et π, π^* deux nombres primaires de $\mathfrak{p}$, $\mathfrak{p}^*$, si l'on a, pour toute unité ξ de $c(\zeta)$,

$$\left\{\frac{\xi}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \xi}{\mathfrak{l}}\right\}, \qquad \left\{\frac{\xi}{\mathfrak{p}^*}\right\} = \left\{\frac{\pi^*, \xi}{\mathfrak{l}}\right\},$$

on a

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\} = \left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}.$$

Démonstration. — $\mathfrak{p}^*$ étant idéal premier de première espèce, nous pouvons déterminer une unité ε de $c(\zeta)$, telle que $\left\{\frac{\varepsilon\pi}{\mathfrak{p}}\right\} = 1$. Considérons alors le corps kummerien $c(\sqrt[l]{\varepsilon\pi}, \zeta)$. Son discriminant relatif ne contenant que les deux facteurs premiers $\mathfrak{l}$ et $\mathfrak{p}$, un nombre $\alpha (\neq 0)$ de $c(\zeta)$ ne possède que les deux caractères

$$\left\{\frac{\alpha, \varepsilon\pi}{\mathfrak{l}}\right\} \quad \text{et} \quad \left\{\frac{\alpha, \varepsilon\pi}{\mathfrak{p}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}.$$

Comme on a $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\} = 1$, $\mathfrak{p}^*$ est décomposable dans $c(\sqrt[l]{\varepsilon\pi}, \zeta)$, soit $\mathfrak{P}$ l'un de ses facteurs premiers dans ce corps.

Pour former les caractères de $\mathfrak{P}^*$, observons que $\mathfrak{p}$ est un idéal premier de première espèce; on peut donc déterminer une unité ε^* de $c(\zeta)$, pour laquelle $\left\{\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right\} = 1$

et $\mathfrak{P}$ possède le caractère unique $\left\{\frac{\varepsilon^*\pi^*,\ \varepsilon\pi}{\mathfrak{l}}\right\}$. Nous concluons alors, du lemme 35, $g \leqq 1$ pour le corps $c(\sqrt[l]{\varepsilon\pi}, \zeta)$, c'est-à-dire que dans ce corps toute classe d'idéaux appartient au genre principal, et le caractère ci-dessus a donc la valeur 1. Or, nous avons $\left(\frac{\varepsilon\pi}{\mathfrak{p}^*}\right) = 1$, c'est-à-dire, à cause de la formule (§ 113),

(142) $$\left(\frac{\mathfrak{p}}{\mathfrak{p}^*}\right) = \left(\frac{\varepsilon}{\mathfrak{p}^*}\right)^{-1};$$

ensuite $\left(\frac{\varepsilon^*\pi^*}{\mathfrak{p}}\right) = 1$, c'est-à-dire

(143) $$\left(\frac{\mathfrak{p}^*}{\mathfrak{p}}\right) = \left(\frac{\varepsilon^*}{\mathfrak{p}}\right)^{-1};$$

et enfin $\left\{\frac{\varepsilon^*\pi^*,\ \varepsilon\pi}{\mathfrak{l}}\right\} = 1$, ou, avec les formules (83),

$$\left\{\frac{\varepsilon^*,\ \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\varepsilon^*,\ \pi}{\mathfrak{l}}\right\}\left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\}\left\{\frac{\pi^*,\ \pi}{\mathfrak{l}}\right\} = 1.$$

Comme (lemme 36) : $\left\{\frac{\varepsilon^*,\ \varepsilon}{\mathfrak{l}}\right\} = 1$, et (lemme 30) : $\left\{\frac{\pi^*,\ \pi^*}{\mathfrak{l}}\right\} = 1$, la dernière formule devient

(144) $$\left\{\frac{\pi,\ \varepsilon^*}{\mathfrak{l}}\right\} = \left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\}.$$

Comme, vu notre hypothèse, on a

$$\left\{\frac{\pi,\ \varepsilon^*}{\mathfrak{l}}\right\} = \left(\frac{\varepsilon^*}{\mathfrak{p}}\right) \quad \text{et} \quad \left\{\frac{\pi^*,\ \varepsilon}{\mathfrak{l}}\right\} = \left(\frac{\varepsilon}{\mathfrak{p}^*}\right),$$

on tire de (144)

$$\left(\frac{\varepsilon^*}{\mathfrak{p}}\right) = \left(\frac{\varepsilon}{\mathfrak{p}^*}\right),$$

égalité qui, jointe aux formules (142), (143), conduit à celle du lemme.

Si l'on veut encore n'appliquer le théorème 151 pour $\mathfrak{w} = \mathfrak{l}$ que si $\alpha \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, on prendra dans la démonstration ci-dessus une unité ε telle que l'on ait, outre $\left(\frac{\varepsilon\pi}{\mathfrak{p}^*}\right) = 1$, $(\varepsilon\pi)^a \equiv 1 + \lambda$, mod $\mathfrak{l}^2$, pour un exposant a premier à l. C'est toujours possible si $\left(\frac{\zeta}{\mathfrak{p}^*}\right) = 1$. Mais si $\left(\frac{\zeta}{\mathfrak{p}^*}\right) \neq 1$ et que $\left(\frac{\pi}{\mathfrak{p}^*}\right) \neq 1$, cette condition peut être vérifiée encore si l'on prend pour ε une puissance convenable de ζ. Il n'y a encore doute que si $\left(\frac{\zeta}{\mathfrak{p}^*}\right) \neq 1$ et $\left(\frac{\pi}{\mathfrak{p}^*}\right) = 1$. Dans ce cas, renversons les rôles de $\mathfrak{p}$, π et $\mathfrak{p}^*$, π^* dans la démonstration : alors il ne reste plus que le cas où l'on aurait en même temps $\left(\frac{\zeta}{\mathfrak{p}^*}\right) \neq 1$, $\left(\frac{\zeta}{\mathfrak{p}}\right) \neq 1$, et $\left(\frac{\pi}{\mathfrak{p}^*}\right) = 1$, $\left(\frac{\pi^*}{\mathfrak{p}}\right) = 1$. Mais dans ce cas les deux dernières conditions montrent sans plus l'exactitude du lemme.

LEMME 40. — $\mathfrak{p}$ étant un idéal premier de première espèce de $c(\zeta)$ et π un nombre primaire de $\mathfrak{p}$, si l'on a pour toute unité ξ de $c(\zeta)$

$$\left\{\frac{\xi}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\,\xi}{\mathfrak{l}}\right\},$$

si, en outre, $\mathfrak{p}^*$ est un idéal premier $\neq\mathfrak{p}$ de première espèce tel que l'on ait

$$\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}\neq 1,$$

il existe toujours dans $c(\zeta)$ une unité ε telle que

$$\left\{\frac{\varepsilon}{\mathfrak{p}^*}\right\}=\left\{\frac{\pi^*,\,\varepsilon}{\mathfrak{l}}\right\}\neq 1,$$

π^* étant un nombre primaire de $\mathfrak{p}^*$.

Démonstration. — Nous procédons exactement comme dans le lemme précédent et nous arrivons, en introduisant certaines unités ε et ε^*, aux trois formules (142), (143), (144). Mais, vu l'hypothèse $\left\{\frac{\varepsilon^*}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\,\varepsilon^*}{\mathfrak{l}}\right\}$, ceci et $\left\{\frac{\mathfrak{p}}{\mathfrak{p}^*}\right\}=\left\{\frac{\mathfrak{p}^*}{\mathfrak{p}}\right\}\neq 1$, ainsi que les trois formules indiquées, conduisent à la démonstration du lemme 40.

Si le théorème 151 n'est admis que dans le cas de $\mu\equiv 1+\lambda$, mod $\mathfrak{l}^2$, il suffit de déterminer ε de manière à vérifier, outre $\left\{\frac{\varepsilon\pi}{\mathfrak{p}^*}\right\}=1$, encore la congruence $(\varepsilon\pi)^a\equiv 1+\lambda$, mod $\mathfrak{l}^2$, avec a premier à l, détermination toujours possible ici.

§ 157. — Cas particulier de la loi de réciprocité pour deux idéaux premiers.

THÉORÈME 162. — $\mathfrak{p}$ et $\mathfrak{q}$ étant deux idéaux premiers quelconques d'un corps circulaire régulier pour lesquels $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\}=1$, on a aussi $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$.

Démonstration. — Soient π, $\varkappa$ des nombres primaires de $\mathfrak{p}$ et $\mathfrak{q}$. Considérons le corps kummerien $c(\sqrt[l]{\pi},\,\zeta)$ et distinguons deux cas, suivant que $\mathfrak{p}$ est de première ou de seconde espèce.

Dans le premier cas, le discriminant relatif de $c(\sqrt[l]{\pi},\,\zeta)$ contient les deux idéaux premiers $\mathfrak{l}$ et $\mathfrak{p}$ et il existe, d'après le lemme 37, une unité ε de $c(\zeta)$ telle que $\left\{\frac{\varepsilon,\,\pi}{\mathfrak{l}}\right\}\neq 1$. Un idéal de $c(\sqrt[l]{\pi},\,\zeta)$ n'a, par suite, qu'un seul caractère, c'est-à-dire que $r=1$ et (lemme 35) $g=1$. Comme $\left\{\frac{\pi}{\mathfrak{q}}\right\}=1$, $\mathfrak{q}$ est décomposable dans $c(\sqrt[l]{\pi},\,\zeta)$; soit $\mathfrak{Q}$ un de ses facteurs premiers. π et $\varkappa$ étant primaires, on a (lemme 30) $\left\{\frac{\varkappa,\,\pi}{\mathfrak{l}}\right\}=1$, et $\mathfrak{Q}$ appartenant au genre principal, on a aussi $\left\{\frac{\varkappa,\,\pi}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\}=1$. C. q. f. d.

Si $\mathfrak{p}$ est de seconde espèce, on a (lemme 37) pour toute unité ξ de $c(\zeta)$: $\left(\frac{\xi,\,\pi}{\mathfrak{l}}\right)=1$, et par suite (démonstration du lemme 37) le discriminant relatif de $c(\sqrt[l]{\pi},\,\zeta)$ ne contient que l'idéal premier $\mathfrak{p}$. Par suite, on a encore $r=1$, $g=1$. $\left(\frac{\pi}{\mathfrak{q}}\right)=1$, donc $\mathfrak{q}$ est décomposable dans $c(\sqrt[l]{\pi},\,\zeta)$. Soit $\mathfrak{Q}$ un de ses facteurs premiers. $\mathfrak{Q}$ étant du genre principal et comme on a $\left(\frac{\xi,\,\pi}{\mathfrak{l}}\right)=1$, on a aussi $\left(\frac{\kappa,\,\pi}{\mathfrak{p}}\right)=\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)=1$. C. q. f. d.

Dans le cas où le théorème 151, et par suite aussi le lemme 35, ne seraient admis pour $\mathfrak{w}=\mathfrak{l}$ que dans le cas de $\mu\equiv 1+\lambda$, mod $\mathfrak{l}^2$, il faut ajouter ce qui suit dans le cas où $\mathfrak{p}$ est de première espèce.

$\mathfrak{p}$ étant un idéal premier quelconque et π un de ses nombres primaires, on déduit de la définition du symbole $\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right)$ (§ 131) et du lemme 24 (§ 132) l'égalité

$$(145)\qquad \left(\frac{\pi,\,\zeta}{\mathfrak{l}}\right)=\zeta^{\frac{n(\mathfrak{p})-1}{l}}=\left(\frac{\zeta}{\mathfrak{p}}\right).$$

Or, si l'idéal premier $\mathfrak{q}$ est tel que l'on ait $\left(\frac{\zeta}{\mathfrak{q}}\right)=1$, déterminons une racine $l^{\text{ième}}$ de l'unité ζ^* telle que l'on ait $\zeta^*\pi^{l-1}\equiv 1+\lambda$, mod $\mathfrak{l}^2$, et envisageons au lieu de $c(\sqrt[l]{\pi},\,\zeta)$ le corps $c(\sqrt[l]{\zeta^*\pi^{l-1}},\,\zeta)$. Nous employons alors la méthode indiquée plus haut. Comme on a

$$\left(\frac{\kappa,\,\zeta^*\pi^{l-1}}{\mathfrak{l}}\right)=\left(\frac{\kappa,\,\zeta^*}{\mathfrak{l}}\right)\left(\frac{\kappa,\,\pi}{\mathfrak{l}}\right)^{l-1},$$

et qu'on a, comme plus haut, $\left(\frac{\kappa,\,\pi}{\mathfrak{l}}\right)=1$; que d'autre part, vu (145), $\left(\frac{\kappa,\,\zeta}{\mathfrak{l}}\right)=\left(\frac{\zeta}{\mathfrak{p}}\right)=1$, il en résulte $\left(\frac{\kappa,\,\zeta^*\pi^{l-1}}{\mathfrak{l}}\right)=1$, et nous en tirons $\left(\frac{\kappa,\,\zeta^*\pi^{l-1}}{\mathfrak{p}}\right)=1$, c'est-à-dire $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)=1$.

Soit, d'autre part, $\left(\frac{\zeta}{\mathfrak{q}}\right)\neq 1$; $\mathfrak{p}$ étant de première espèce, il existe sûrement une unité ε_1 telle que $\left(\frac{\varepsilon_1}{\mathfrak{p}}\right)\neq 1$, et de plus (lemme 37) une unité ε_2 telle que $\left(\frac{\varepsilon_2,\,\pi}{\mathfrak{l}}\right)\neq 1$. On peut, de plus, choisir ces unités $\equiv 1+\lambda$, mod. $\mathfrak{l}^2$. Nous en déduisons l'existence d'une unité ε, pour laquelle $\left(\frac{\varepsilon}{\mathfrak{p}}\right)\neq 1$ et $\left(\frac{\varepsilon,\,\pi}{\mathfrak{l}}\right)\neq 1$, et telle que $\varepsilon\equiv 1+\lambda$, mod $\mathfrak{l}^2$. En effet, si ces conditions ne sont remplies ni par ε_1 ni par ε_2, on a simultanément $\left(\frac{\varepsilon_1,\,\pi}{\mathfrak{l}}\right)=1$, $\left(\frac{\varepsilon_2}{\mathfrak{p}}\right)=1$, et alors $\varepsilon=(\varepsilon_1\varepsilon_2)^{\frac{l-1}{2}}$ serait une unité vérifiant ces conditions. Déterminons alors une puissance $\eta=\varepsilon^a$ de ε telle que l'on ait $\left(\frac{\eta\kappa}{\mathfrak{p}}\right)=1$. Si l'on avait $\left(\frac{\kappa}{\mathfrak{p}}\right)\neq 1$, a serait sûrement premier à l et on aurait $\left(\frac{\eta,\,\pi}{\mathfrak{l}}\right)\neq 1$.

De plus, κ étant primaire, il est visible qu'une certaine puissance de $\eta\kappa$ d'expo-

sant premier à l est congrue à $1+\lambda$, mod $\mathfrak{l}^2$. De (145) et du lemme 36 résulte encore $\left\{\frac{\zeta,\,\eta\varkappa}{\mathfrak{l}}\right\} \neq 1$. Le corps kummerien $c(\sqrt[l]{\eta\varkappa},\,\zeta)$ ne possède donc qu'un genre. Comme $\left\{\frac{\eta\varkappa}{\mathfrak{p}}\right\} = 1$, $\mathfrak{p}$ est décomposable dans ce corps; $\mathfrak{P}$ étant un de ses facteurs premiers, son caractère est égal au symbole

$$\left\{\frac{\zeta^*\pi,\,\eta\varkappa}{\mathfrak{q}}\right\} = \left\{\frac{\zeta^*\pi}{\mathfrak{q}}\right\},$$

ζ^* étant une racine $l^{\text{ième}}$ de l'unité telle que l'on ait $\left\{\frac{\zeta^*\pi,\,\eta\varkappa}{\mathfrak{l}}\right\} = 1$. Vu la dernière égalité et comme on a $\left\{\frac{\zeta,\,\eta}{\mathfrak{l}}\right\} = 1$, il en résulte $\left\{\frac{\zeta^*,\,\varkappa}{\mathfrak{l}}\right\}\left\{\frac{\pi,\,\eta}{\mathfrak{l}}\right\} = 1$, et, à cause de $\left\{\frac{\pi,\,\eta}{\mathfrak{l}}\right\} = 1$, $\left\{\frac{\zeta^*,\,\varkappa}{\mathfrak{l}}\right\}$ est aussi $\neq 1$, c'est-à-dire, vu (145), $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} \neq 1$; on a donc $\zeta^* \neq 1$. Mais comme l'un des caractères de l'idéal premier $\mathfrak{P}$ doit être égal à 1, il résulte de $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$ nécessairement $\left\{\frac{\zeta^*}{\mathfrak{q}}\right\} = 1$, contrairement à ce qui précède.

§ 158. — Existence d'idéaux premiers auxiliaires pour lesquels la loi de réciprocité se vérifie.

Lemme 41. — $\mathfrak{p}$ étant un idéal premier quelconque du corps circulaire régulier $c(\zeta)$, il existe toujours dans $c(\zeta)$ un idéal premier $\mathfrak{r}$ vérifiant les conditions

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\} \neq 1, \qquad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1.$$

Démonstration. — Soit h le nombre de classes de $c(\zeta)$ et, comme aux paragraphes 149 et 154, h^* un entier positif tel que l'on ait $hh^* \equiv 1$, mod l. Soit p le nombre premier divisible par $\mathfrak{p}$ et $\pi = \mathfrak{p}^{hh^*}$ un nombre primaire de $\mathfrak{p}$; soient, de plus, $\mathfrak{p}'$, $\mathfrak{p}''$, ... les idéaux premiers distincts conjugués de $\mathfrak{p}$ dans $c(\zeta)$ et $\pi' = \mathfrak{p}'^{hh^*}$, $\pi'' = \mathfrak{p}''^{hh^*}$, etc., les conjugués de π dans $c(\zeta)$: ils sont primaires pour $\mathfrak{p}'$, $\mathfrak{p}''$, ... On a ensuite $p = \mathfrak{p}\mathfrak{p}'\mathfrak{p}''\ldots$. Comme, de plus, $\frac{p^{hh^*}}{\pi\pi'\pi''\ldots}$ doit être une unité de $c(\zeta)$ et que c'est un nombre primaire, il résulte du théorème 156 (voir aussi § 142) que ce quotient représente la $l^{\text{ème}}$ puissance d'une unité ε de $c(\zeta)$:

$$p^{hh^*} = \varepsilon^l \pi\pi'\pi''\ldots .$$

Appliquons alors le théorème 152, en prenant

$$\alpha_1 = \zeta, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \quad \ldots,$$

$$\gamma_1 = \zeta, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \quad \ldots.$$

ε n'étant pas la $l^{\text{ième}}$ puissance d'une unité de $c(\zeta)$ et π, π', π'', ... étant des puissances d'idéaux premiers dont les exposants sont premiers à l, les conditions du théorème 152 sont remplies, et il existe par suite dans $c(\zeta)$ un idéal premier $\mathfrak{r}$ et un certain exposant m premier à l tel que l'on ait

$$\left\{\frac{\varepsilon}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi}{\mathfrak{r}}\right\}^m = \zeta, \quad \left\{\frac{\pi'}{\mathfrak{r}}\right\}^m = 1, \quad \left\{\frac{\pi''}{\mathfrak{r}}\right\}^m = 1, \quad \ldots,$$

c'est-à-dire

$$(146) \qquad \left\{\frac{\zeta}{\mathfrak{r}}\right\} = \zeta^*, \quad \left\{\frac{\pi}{\mathfrak{r}}\right\} = \zeta^*, \quad \left\{\frac{\pi'}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\pi''}{\mathfrak{r}}\right\} = 1, \quad \ldots,$$

où ζ^* est une racine $l^{\text{ième}}$ de l'unité autre que 1.

De (146), on tire $\left\{\frac{p^{hh}}{\mathfrak{r}}\right\} = \left\{\frac{\varepsilon^{-l}p^{hh}}{\mathfrak{r}}\right\} = \left\{\frac{\pi\pi'\pi''\ldots}{\mathfrak{r}}\right\} = \zeta^*$, et par suite on a aussi, vu le théorème 140, $\left\{\frac{\rho}{p^{hh}}\right\} = \zeta^*$, ρ étant un nombre primaire de $\mathfrak{r}$. Comme maintenant, vu (146) et le théorème 162, on doit avoir $\left\{\frac{\rho}{\pi'}\right\} = 1$, $\left\{\frac{\rho}{\pi''}\right\} = 1$, ... et que

$$\left\{\frac{\rho}{p^{hh}}\right\} = \left\{\frac{\rho}{\pi}\right\}\left\{\frac{\rho}{\pi'}\right\}\left\{\frac{\rho}{\pi''}\right\}\ldots,$$

nous obtenons

$$\left\{\frac{\rho}{\pi}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} = \zeta^*. \qquad \text{C. q. f. d.}$$

LEMME 42. — $\mathfrak{p}$ étant un idéal premier quelconque du corps circulaire régulier $c(\zeta)$ et π un de ses nombres primaires, ε étant une unité quelconque de $c(\zeta)$ non égale toutefois à la $l^{\text{ième}}$ puissance d'une unité de $c(\zeta)$, il existe toujours dans $c(\zeta)$ un idéal premier $\mathfrak{r}$ vérifiant les conditions

$$\left\{\frac{\varepsilon\pi}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\} \neq 1.$$

Démonstration. — Soient π, π', π'', ... les mêmes nombres que dans la démonstration précédente; prenons pour le théorème 152

$$\alpha_1 = \varepsilon\pi, \quad \alpha_2 = \pi, \quad \alpha_3 = \pi', \quad \alpha_4 = \pi'', \quad \alpha_5 = \pi''', \quad \ldots,$$
$$\gamma_1 = 1, \quad \gamma_2 = \zeta, \quad \gamma_3 = 1, \quad \gamma_4 = 1, \quad \gamma_5 = 1, \quad \ldots,$$

les nombres α_1, α_2, ... vérifiant encore les conditions du théorème 152. Une démonstration semblable à la précédente conduit à un idéal premier $\mathfrak{r}$ remplissant les conditions de l'énoncé.

§ 159. — Démonstration de la première loi complémentaire.

Pour démontrer la première loi complémentaire dans le cas d'un idéal premier $\mathfrak{p}$ de première espèce, appliquons le lemme 41 ; on peut déterminer un idéal premier $\mathfrak{r}$ tel que l'on ait

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}=1 \quad \text{et} \quad \left\{\frac{\mathfrak{r}}{\mathfrak{p}}\right\}=\left\{\frac{\mathfrak{p}}{\mathfrak{r}}\right\}=1,$$

et que, par suite, il soit de la première espèce. D'après (145), on a pour l'idéal $\mathfrak{r}$ l'égalité

$$\left\{\frac{\zeta}{\mathfrak{r}}\right\}=\zeta^{\frac{n(\mathfrak{r})-1}{l}}=\left\{\frac{\rho,\zeta}{\mathfrak{l}}\right\},$$

ρ étant un nombre primaire de $\mathfrak{r}$. Comme on a $\left\{\frac{\zeta}{\mathfrak{r}}\right\}=1$, on a pour toute autre unité ξ de $c(\zeta)$ (lemme 38)

$$\left\{\frac{\xi}{\mathfrak{r}}\right\}=\left\{\frac{\rho,\xi}{\mathfrak{l}}\right\},$$

et par conséquent les conditions du lemme 40 sont remplies par les idéaux $\mathfrak{r}$ et $\mathfrak{p}$. D'après ce lemme, il existe donc dans $c(\zeta)$ une unité ε telle que l'on ait

$$\left\{\frac{\varepsilon}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\varepsilon}{\mathfrak{l}}\right\}=1,$$

π étant un nombre primaire de $\mathfrak{p}$. Par suite, on a (lemme 38) pour toute autre unité ξ de $c(\zeta)$ l'égalité $\left\{\frac{\xi}{\mathfrak{p}}\right\}=\left\{\frac{\pi,\xi}{\mathfrak{l}}\right\}$, ce qui démontre la première loi complémentaire de la loi de réciprocité si $\mathfrak{p}$ est de première espèce.

Soit maintenant $\mathfrak{q}$ idéal premier de deuxième espèce de $c(\zeta)$. Alors on a, pour toute unité ξ de $c(\zeta)$, $\left\{\frac{\xi}{\mathfrak{q}}\right\}=1$, et $\varkappa$ étant un nombre primaire de $\mathfrak{q}$, on a toujours aussi (lemme 37) $\left\{\frac{\varkappa,\xi}{\mathfrak{l}}\right\}=1$. On a donc encore la première loi complémentaire

$$\left\{\frac{\xi}{\mathfrak{q}}\right\}=\left\{\frac{\varkappa,\xi}{\mathfrak{l}}\right\}.$$

§ 160. — Démonstration de la loi de réciprocité entre deux idéaux premiers quelconques.

La première loi complémentaire ayant été démontrée, on en conclut, avec le lemme 39, la loi de réciprocité pour deux idéaux premiers quelconques de première espèce.

Soient, *en second lieu*, $\mathfrak{p}$ un idéal premier de deuxième espèce, π et $\varkappa$ des nombres primaires de $\mathfrak{p}$ et $\mathfrak{q}$. Dans le cas où l'on a $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = 1$, il résulte du théorème 162 $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = 1$, et par suite l'exactitude de la loi de réciprocité pour $\mathfrak{p}$ et $\mathfrak{q}$. Supposons maintenant $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = \left(\frac{\varkappa}{\mathfrak{p}}\right) \neq 1$. $\mathfrak{p}$ étant de première espèce, il existe une unité ε telle que $\left(\frac{\varepsilon\varkappa}{\mathfrak{p}}\right) = 1$, et on peut de plus toujours supposer qu'une certaine puissance de $\varepsilon\varkappa$, d'exposant premier à l, est $\equiv 1 + \lambda$, mod $\mathfrak{l}^2$ (cela ressort d'une considération à la fin de la démonstration du lemme 39). Considérons le corps kummerien $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$. D'après le théorème 148, le discriminant relatif de ce corps par rapport à $c(\zeta)$ contient les deux facteurs premiers $\mathfrak{l}$ et $\mathfrak{q}$; $\mathfrak{q}$ étant de deuxième espèce, on a, vu les lemmes 36 et 37, pour toute unité ξ de $c(\zeta)$

$$\left(\frac{\xi,\ \varepsilon\varkappa}{\mathfrak{l}}\right) = \left(\frac{\xi,\ \varepsilon}{\mathfrak{l}}\right)\left(\frac{\xi,\ \varkappa}{\mathfrak{l}}\right) = 1, \qquad \left(\frac{\xi}{\mathfrak{q}}\right) = 1,$$

et, d'après cela, le nombre des caractères distinctifs du genre d'un idéal de $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ est égal à 2. D'après le lemme 35 le nombre des genres de ce corps est donc $g \leq l$. Déterminons alors, d'après le lemme 42, un idéal premier $\mathfrak{r}$ de $c(\zeta)$ tel que l'on ait

$$\left(\frac{\varepsilon\varkappa}{\mathfrak{r}}\right) = 1, \qquad \left(\frac{\mathfrak{r}}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{q}}{\mathfrak{r}}\right) \neq 1.$$

A cause de la première égalité, $\mathfrak{r}$ est encore décomposable dans $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$. Soit $\mathfrak{R}$ un de ses facteurs premiers dans ce corps et ρ un de ses nombres primaires. L'idéal $\mathfrak{R}$ a dès lors dans $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ les deux caractères

(147) $$\left(\frac{\rho,\ \varepsilon\varkappa}{\mathfrak{l}}\right), \qquad \left(\frac{\rho,\ \varepsilon\varkappa}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{r}}{\mathfrak{q}}\right).$$

Comme le second caractère est $\neq 1$, les idéaux $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ déterminent des genres tous différents, et il n'y en a pas d'autres, vu la limite supérieure trouvée pour g. En appliquant la première loi complémentaire (§ 159), on obtient

$$\left(\frac{\rho,\ \varepsilon\varkappa}{\mathfrak{l}}\right)\left(\frac{\mathfrak{r}}{\mathfrak{q}}\right) = \left(\frac{\rho,\ \varepsilon}{\mathfrak{l}}\right)\left(\frac{\mathfrak{r}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon}{\mathfrak{r}}\right)\left(\frac{\mathfrak{r}}{\mathfrak{q}}\right) = \left(\frac{\varepsilon}{\mathfrak{r}}\right)\left(\frac{\mathfrak{q}}{\mathfrak{r}}\right) = \left(\frac{\varepsilon\varkappa}{\mathfrak{r}}\right) = 1.$$

C'est-à-dire que le produit des deux caractères (147) est égal à 1. Comme tout idéal de $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ appartient à l'un des l genres, il en résulte que tout idéal de $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$ a deux caractères de produit égal à 1. A cause de $\left(\frac{\varepsilon\varkappa}{\mathfrak{p}}\right) = 1$, $\mathfrak{p}$ est encore décomposable dans $c(\sqrt[l]{\varepsilon\varkappa}, \zeta)$; soit $\mathfrak{P}$ un de ses facteurs premiers dans ce corps; les deux caractères de cet idéal sont les symboles

$$\left(\frac{\pi,\ \varepsilon\varkappa}{\mathfrak{l}}\right), \qquad \left(\frac{\pi,\ \varepsilon\varkappa}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right).$$

et on en conclut, d'après la première loi complémentaire,

$$\left(\frac{\pi,\ \varepsilon\varkappa}{\mathfrak{l}}\right)\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=\left(\frac{\pi,\ \varepsilon}{\mathfrak{l}}\right)\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=\left(\frac{\varepsilon}{\mathfrak{p}}\right)\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=1,$$

ou

$$\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right)=\left(\frac{\varepsilon}{\mathfrak{p}}\right)^{-1}=\left(\frac{\varkappa}{\mathfrak{p}}\right)=\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right),$$

ce qui démontre la loi de réciprocité pour les idéaux $\mathfrak{p}$ et $\mathfrak{q}$.

Soient, *en troisième lieu*, $\mathfrak{q}$ et $\mathfrak{q}^*$ deux idéaux premiers de deuxième espèce, $\varkappa$, $\varkappa^*$ des nombres primaires de $\mathfrak{q}$, $\mathfrak{q}^*$. Considérons le corps kummerien $c\left(\sqrt[l]{\varkappa\varkappa^*},\ \zeta\right)$. Les nombres $\varkappa$ et $\varkappa^*$ sont, on l'a vu dans la démonstration du lemme 37, congrus mod $\mathfrak{l}^2$ à des $l^{\text{ièmes}}$ puissances de nombres de $c(\zeta)$; il en est donc de même de $\varkappa\varkappa^*$, et par suite, d'après le théorème 148, le discriminant relatif du corps $c\left(\sqrt[l]{\varkappa\varkappa^*},\ \zeta\right)$ n'est pas divisible par $\mathfrak{l}$. Ce discriminant relatif ne contient, par suite, que les deux facteurs premiers $\mathfrak{q}$ et $\mathfrak{q}^*$. Or, on a pour toute unité ξ de $c(\zeta)$

$$\left(\frac{\xi,\ \varkappa\varkappa^*}{\mathfrak{q}}\right)=\left(\frac{\xi}{\mathfrak{q}}\right)=1,\qquad \left(\frac{\xi,\ \varkappa\varkappa^*}{\mathfrak{q}^*}\right)=\left(\frac{\xi}{\mathfrak{q}^*}\right)=1,$$

et par suite le nombre des caractères distinctifs des genres de $c\left(\sqrt[l]{\varkappa\varkappa^*},\ \zeta\right)$ est $r=2$. D'après le lemme 35, on a alors $g\leqq l$. Ensuite, d'après le théorème 152, on peut toujours déterminer un idéal premier $\mathfrak{r}$ de $c(\zeta)$ tel que l'on ait

$$\left(\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right)=1,\qquad \left(\frac{\zeta}{\mathfrak{r}}\right)=1,\qquad \left(\frac{\varkappa}{\mathfrak{r}}\right)\neq 1.$$

$\mathfrak{r}$ est encore décomposable dans $c(\zeta)$. Soit $\mathfrak{R}$ un de ses facteurs premiers, ρ un de ses nombres primaires. Les caractères de l'idéal $\mathfrak{R}$ dans le corps kummerien sont les deux symboles

$$(148)\qquad \begin{cases} \left(\dfrac{\rho,\ \varkappa\varkappa^*}{\mathfrak{q}}\right)=\left(\dfrac{\rho}{\mathfrak{q}}\right)=\left(\dfrac{\mathfrak{r}}{\mathfrak{q}}\right), \\[2ex] \left(\dfrac{\rho,\ \varkappa\varkappa^*}{\mathfrak{q}^*}\right)=\left(\dfrac{\rho}{\mathfrak{q}^*}\right)=\left(\dfrac{\mathfrak{r}}{\mathfrak{q}^*}\right). \end{cases}$$

Comme le premier caractère est, d'après le théorème 162, nécessairement $\neq 1$, puisque $\left(\frac{\varkappa}{\mathfrak{r}}\right)\neq 1$, les idéaux $\mathfrak{R}$, $\mathfrak{R}^2$, …, $\mathfrak{R}^l$ déterminent l genres distincts et il n'y en a pas d'autres. Comme on a $\left(\frac{\zeta}{\mathfrak{r}}\right)=1$, $\mathfrak{r}$ est un idéal de première espèce; par suite, d'après ce qui précède, la loi de réciprocité s'applique d'une part à $\mathfrak{r}$, $\mathfrak{q}$; d'autre part à $\mathfrak{r}$, $\mathfrak{q}^*$, et le produit des deux caractères (148) est donc

$$(149)\qquad \left(\frac{\mathfrak{r}}{\mathfrak{q}}\right)\left(\frac{\mathfrak{r}}{\mathfrak{q}^*}\right)=\left(\frac{\mathfrak{q}}{\mathfrak{r}}\right)\left(\frac{\mathfrak{q}^*}{\mathfrak{r}}\right)=\left(\frac{\varkappa\varkappa^*}{\mathfrak{r}}\right)=1.$$

Comme tout idéal de $c(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$ appartient à un des l genres, il résulte de (149) que tout idéal a deux caractères dont le produit est égal à 1. Or, l'idéal $\mathfrak{q}$ est égal à la $l^{\text{ème}}$ puissance d'un idéal premier $\mathfrak{Q}$ de $c(\sqrt[l]{\varkappa\varkappa^*}, \zeta)$. Les deux caractères de $\mathfrak{Q}$ dans ce corps sont alors

$$\left\{\frac{\varkappa, \varkappa\varkappa^*}{\mathfrak{q}}\right\} = \left\{\frac{\varkappa^*, \varkappa\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\varkappa^*}{\mathfrak{q}}\right\}^{-1} = \left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\}^{-1}, \qquad \left\{\frac{\varkappa, \varkappa\varkappa^*}{\mathfrak{q}^*}\right\} = \left\{\frac{\varkappa}{\mathfrak{q}^*}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\},$$

et leur produit devant être égal à 1, on obtient

$$\left\{\frac{\mathfrak{q}^*}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\mathfrak{q}^*}\right\}.$$

La loi de réciprocité est ainsi démontrée pour deux idéaux premiers quelconques.

§ 161. — Démonstration de la deuxième loi complémentaire.

Soit d'abord $\mathfrak{p}$ un idéal premier de première espèce et π un nombre primaire de $\mathfrak{p}$. Déterminons une unité ε de $c(\zeta)$, telle que l'on ait $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$, et considérons le corps kummerien $c(\sqrt[l]{\varepsilon\lambda}, \zeta)$. Comme $\left\{\frac{\varepsilon\lambda}{\mathfrak{p}}\right\} = 1$, $\mathfrak{p}$ est encore décomposable dans ce corps; soit $\mathfrak{P}$ un de ses facteurs premiers. Nous voyons que l'idéal $\mathfrak{P}$ a un seul caractère, $\left\{\frac{\pi, \varepsilon\lambda}{\mathfrak{l}}\right\}$; et comme il n'y a aussi qu'un genre (lemme 35), le genre principal, ce caractère doit être égal à 1. Par suite, comme (§ 159) $\left\{\frac{\varepsilon}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \varepsilon}{\mathfrak{l}}\right\}$, on a de suite l'égalité

$$\left\{\frac{\lambda}{\mathfrak{p}}\right\} = \left\{\frac{\pi, \lambda}{\mathfrak{l}}\right\}.$$

Soit, en second lieu, $\mathfrak{q}$ un idéal premier de seconde espèce, et $\varkappa$ un nombre primaire de $\mathfrak{q}$; il y a deux cas à distinguer, suivant que l'on a $\left\{\frac{\lambda}{\mathfrak{q}}\right\} = 1$ ou $\neq 1$. Dans le premier cas, la considération du corps kummerien $c(\sqrt[l]{\lambda}, \zeta)$ montre que l'on a aussi $\left\{\frac{\varkappa, \lambda}{\mathfrak{l}}\right\} = 1$. Dans le second cas, on déterminera, d'après le théorème 152, un idéal premier $\mathfrak{p}$, pour lequel on ait $\left\{\frac{\zeta}{\mathfrak{p}}\right\} = \left\{\frac{\varkappa}{\mathfrak{p}}\right\} \neq 1$. Alors $\mathfrak{p}$ est nécessairement de première espèce, et il résulte du théorème 162, π étant un nombre primaire de $\mathfrak{p}$, $\left\{\frac{\pi}{\mathfrak{q}}\right\} \neq 1$; on peut donc déterminer un entier rationnel a de façon que $\left\{\frac{\lambda\pi^a}{\mathfrak{q}}\right\} = 1$. En considérant le corps $c(\sqrt[l]{\lambda\pi^a}, \zeta)$, comme on a $\left\{\frac{\zeta^a, \lambda\pi^a}{\mathfrak{p}}\right\} = \left\{\frac{\zeta^a}{\mathfrak{p}}\right\} \neq 1$, un idéal n'a encore dans ce corps qu'un seul caractère, toujours égal à 1. Appliquant ceci à un

facteur premier $\mathfrak{Q}$ de $\mathfrak{q}$ dans ce corps, on a $\left(\frac{\zeta\kappa,\ \lambda\pi^{a}}{\mathfrak{l}}\right) = \left(\frac{\zeta}{\mathfrak{p}}\right)^{a}\left(\frac{\kappa,\ \lambda}{\mathfrak{l}}\right) = 1$, et en tenant compte de l'égalité $\left(\frac{\mathfrak{p}}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)$, on a $\left(\frac{\lambda}{\mathfrak{q}}\right) = \left(\frac{\kappa,\ \lambda}{\mathfrak{l}}\right)$.

C'est Kummer qui a démontré le premier la loi de réciprocité des résidus de puissances $l^{\text{ièmes}}$. Notre démonstration nouvelle diffère de celle de Kummer, surtout en ce que Kummer obtient d'abord la première loi complémentaire, au moyen de calculs considérables, par une généralisation très habile des formules de la division du cercle, et que c'est seulement alors en s'appuyant sur ces calculs, qu'il en déduit la loi de réciprocité entre deux idéaux premiers; au contraire, dans les développements qui précèdent, les démonstrations de la loi de réciprocité et des deux lois complémentaires découlent d'une source commune.

Parmi les lois de réciprocité particulière que l'on traite à l'aide des formules de la division du cercle, citons la loi de réciprocité des résidus biquadratiques [Gauss[3], Eisenstein[8, 9]], celle des résidus cubiques [Eisenstein[5, 7], Jacobi[1]], puis les recherches de Gmeiner[1, 2, 3] pour les résidus bicubiques et celles de Jacobi[4] pour les restes de puissances 5e, 8e et 12e.

Mentionnons aussi que Eisenstein a donné sans démonstration une loi de réciprocité pour les restes de $l^{\text{ièmes}}$ puissances et a même envisagé le cas où le nombre des classes du corps circulaire des racines $l^{\text{ièmes}}$ de l'unité est divisible par l. [Eisenstein[1, 12].]

CHAPITRE XXXIV.

Nombre des genres d'un corps kummerien régulier.

§ 162. — Théorème sur le symbole $\left(\frac{\nu,\ \mu}{\mathfrak{w}}\right)$.

Théorème 163. — ν et μ étant deux entiers quelconques $\neq 0$ d'un corps circulaire régulier $c(\zeta)$, on a toujours

$$\prod_{(\mathfrak{w})}\left(\frac{\nu,\ \mu}{\mathfrak{w}}\right) = 1,$$

le produit étant étendu à tous les idéaux premiers $\mathfrak{w}$ de $c(\zeta)$.

Démonstration. — Soit h le nombre des classes d'idéaux de $c(\zeta)$ et h^* un entier positif tel que $hh^* \equiv 1$, mod l. Posons $\nu = \mathfrak{l}^{a}\mathfrak{p}_1\mathfrak{p}_2\ldots$ et $\mu = \mathfrak{l}^{b}\mathfrak{q}_1\mathfrak{q}_2\ldots$, a et b étant des exposants entiers et $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$ des idéaux premiers déterminés de

$c(\zeta)$. $\pi_1, \pi_2, \ldots, \varkappa_1, \varkappa_2, \ldots$ étant des nombres primaires des idéaux premiers $\mathfrak{p}_1$, $\mathfrak{p}_2, \ldots, \mathfrak{q}_1, \mathfrak{q}_2, \ldots$ et tels que l'on ait

$$\pi_1 = \mathfrak{p}_1^{hh}, \quad \pi_2 = \mathfrak{p}_2^{hh}, \quad \ldots, \quad \varkappa_1 = \mathfrak{q}_1^{hh}, \quad \varkappa_2 = \mathfrak{q}_2^{hh}, \quad \ldots$$

on a, en posant $\lambda = 1 - \zeta$,

(150) $$\nu^{hh} = \varepsilon\lambda^{ahh}\pi_1\pi_2\ldots, \quad \mu^{hh} = \eta\lambda^{bhh}\varkappa_1\varkappa_2\ldots,$$

ε et η étant des unités de $c(\zeta)$. $\mathfrak{w}$ étant un idéal premier quelconque, on a toujours

(151) $$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = \left(\frac{\nu^{hh}, \mu^{hh}}{\mathfrak{w}}\right).$$

Soient alors $\mathfrak{p}$, $\mathfrak{q}$ deux idéaux premiers distincts autres que $\mathfrak{l}$ de $c(\zeta)$ et π, $\varkappa$ deux nombres primaires correspondants; soient, de plus, ε, η des unités quelconques de $c(\zeta)$. On tire facilement du lemme 36 et du théorème 161 les formules

(152) $$\begin{cases} \left(\frac{\varepsilon, \eta}{\mathfrak{l}}\right) = 1, & \left(\frac{\varepsilon, \lambda}{\mathfrak{l}}\right) = 1, \\ \left(\frac{\varepsilon, \pi}{\mathfrak{l}}\right)\left(\frac{\varepsilon, \pi}{\mathfrak{p}}\right) = 1, & \left(\frac{\pi, \varkappa}{\mathfrak{p}}\right)\left(\frac{\pi, \varkappa}{\mathfrak{q}}\right) = 1. \end{cases}$$

$\mathfrak{w}$ étant un idéal premier autre que $\mathfrak{l}$, non diviseur de μ, le discriminant relatif du corps kummerien $c(\sqrt[l]{\mu}, \zeta)$ est (théorème 148) premier à $\mathfrak{w}$; si $\mathfrak{w}$ est aussi premier à ν, ν est résidu de normes du corps kummérien $c(\sqrt[l]{\mu}, \zeta)$ (théorème 150) et on a, par suite (théorème 151), $\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1$. Par suite (vu 152) le théorème est vrai si l'un des deux nombres ν, μ est soit une unité, soit une puissance quelconque de λ, soit un nombre primaire d'un idéal premier $\neq \mathfrak{l}$; à cause de (150) et (151) et des règles (80) et (83), le théorème 163 est donc général.

§ 163. — Théorème fondamental sur les genres d'un corps kummerien régulier.

Théorème 164. — *Soit r le nombre des caractères distinctifs d'un genre du corps kummerien régulier $C = c(\sqrt[l]{\mu}, \zeta)$; pour qu'un système donné de r racines $l^{\text{èmes}}$ de l'unité caractérise un genre de C, il faut et il suffit que le produit de ces r caractères soit égal à 1. Le nombre des genres de C est par suite l^{r-1}.*

Démonstration. — Soit h le nombre de classes du corps circulaire régulier $c(\zeta)$, h^* un entier positif, tel que l'on ait $hh^* \equiv 1$, mod l; soient $\mathfrak{l}_1, \ldots, \mathfrak{l}_r$ les r facteurs premiers du discriminant relatif de C choisis conformément au paragraphe 149. Soit A une classe d'idéaux quelconque de C, $\mathfrak{J}$ un de ses idéaux premier à $\mathfrak{l} = 1 - \zeta$

et au discriminant relatif de C; soit $\bar{\nu} = (N_c[\mathfrak{J}])^{hh'}$ l'entier de $c(\zeta)$, formé selon le paragraphe 149 et pourvu d'un certain facteur unité de telle sorte que

$$\chi_1(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_1}\right\}, \quad \ldots, \quad \chi_r(\mathfrak{J}) = \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_r}\right\};$$

soient les r caractères distinctifs du genre de $\mathfrak{J}$. Soit $\mathfrak{p}$ un idéal de $c(\zeta)$, dans le cas où il en existe un, figurant dans $\bar{\nu}$ avec un exposant divisible par l; $\mathfrak{p}$ est alors sûrement différent de $\mathfrak{l}$ et premier au discriminant relatif de C. $N_c(\mathfrak{J})$ étant la norme relative d'un idéal, $\mathfrak{p}$ doit être décomposable dans C. On a donc (théorème 149) pour un tel idéal $\mathfrak{p}$: $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$, et par suite aussi $\left\{\frac{\bar{\nu}, \mu}{\mathfrak{p}}\right\} = 1$. Vu le théorème 163, il en résulte

$$\prod_{(\mathfrak{w})} \left\{\frac{\bar{\nu}, \mu}{\mathfrak{w}}\right\} = 1, \tag{153}$$

le produit étant étendu à tous les facteurs idéaux premiers $\mathfrak{w}$ distincts de $\mathfrak{l}$ du discriminant relatif de C et, en outre, à l'idéal premier $\mathfrak{l}$. Ensuite on a, $\mathfrak{l}_{r+1}, \ldots, \mathfrak{l}_t$ étant les autres facteurs premiers du discriminant relatif, vu le paragraphe 149 :

$$\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+1}}\right\} = 1, \quad \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_{r+2}}\right\} = 1, \quad \ldots, \quad \left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}_t}\right\} = 1. \tag{154}$$

Si alors le discriminant relatif du corps C contient l'idéal premier $\mathfrak{l}$, (153) montre déjà que le produit des r caractères est égal à 1. Dans le cas contraire, le nombre $\bar{\nu}$ est (théorème 150) résidu de normes du corps C, mod $\mathfrak{l}$, et par suite (théorème 151) $\left\{\frac{\bar{\nu}, \mu}{\mathfrak{l}}\right\} = 1$; on voit encore dans ce cas, d'après (153) et (154), l'exactitude de l'une des parties du théorème 164.

Pour abréger, nous ne démontrerons la seconde partie que dans le cas où le discriminant relatif de C ne contient pas $\mathfrak{l}$. Soient alors encore $\mathfrak{l}_1, \ldots, \mathfrak{l}_t$ ses facteurs premiers dans $c(\zeta)$ et $\lambda_1, \ldots, \lambda_t$ des nombres primaires correspondants; soit e_i l'exposant de $\mathfrak{l}_i$ dans μ et e_i^* un entier tel que $e_i e_i^* \equiv 1$, mod l. Enfin, soient $\gamma_1, \ldots, \gamma_r$, r racines $l^{\text{èmes}}$ de l'unité quelconques dont le produit $\gamma_1 \ldots \gamma_r = 1$; d'après le théorème 152, il existe alors toujours dans $c(\zeta)$ un idéal premier $\mathfrak{p}$ non diviseur de μ et remplissant les conditions

$$\left\{\frac{\lambda_1}{\mathfrak{p}}\right\}^m = \gamma_1^{e_1}, \quad \left\{\frac{\lambda_2}{\mathfrak{p}}\right\}^m = \gamma_2^{e_2}, \quad \ldots, \quad \left\{\frac{\lambda_r}{\mathfrak{p}}\right\}^m = \gamma_r^{e_r}, \tag{155}$$

$$\left\{\frac{\lambda_{r+1}}{\mathfrak{p}}\right\}^m = 1, \quad \left\{\frac{\lambda_{r+2}}{\mathfrak{p}}\right\}^m = 1, \quad \ldots, \quad \left\{\frac{\lambda_t}{\mathfrak{p}}\right\}^m = 1 \tag{156}$$

pour un exposant m de la série $1, 2, \ldots, l-1$. π étant un nombre primaire de $\mathfrak{p}$, on a, vu (155), d'après le théorème 161,

$$\left\{\frac{\pi^m, \mu}{\mathfrak{l}_t}\right\} = \left\{\frac{\pi, \mu}{\mathfrak{l}_t}\right\}^m = \left\{\frac{\pi}{\mathfrak{l}_t}\right\}^{me_t} = \left\{\frac{\lambda_t}{\mathfrak{p}}\right\}^{me_t} = \gamma_t. \tag{157}$$

$$(t = 1, 2, \ldots, r)$$

On obtient de même, vu (156),

$$(158)\qquad \left(\frac{\nu, \mu}{\mathfrak{l}_u}\right) = \left(\frac{\nu}{\mathfrak{l}_u}\right)^{e_u} = \left(\frac{\lambda_u}{\mathfrak{p}}\right)^{e_u} = 1, \quad (u = r+1, r+2, \dots, t)$$

Comme $\gamma_1 \gamma_2 \dots \gamma_t = 1$, on a, vu (157) et (158),

$$(159)\qquad \prod_{(\mathfrak{w})} \left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1,$$

le produit étant étendu à tous les idéaux premiers $\mathfrak{l}_1, \dots, \mathfrak{l}_t$. Si alors $\mathfrak{w}$ est un idéal premier de $c(\zeta)$ autre que $\mathfrak{p}, \mathfrak{l}_1, \dots, \mathfrak{l}_t$, le nombre ν (théorème 150) est reste de normes du corps kummerien, mod $\mathfrak{w}$, et par suite (théorème 151) on a toujours $\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1$. On tire de là et de (159) et du théorème 163 que l'on a aussi $\left(\frac{\nu, \mu}{\mathfrak{p}}\right) = 1$, c'est-à-dire $\left(\frac{\mu}{\mathfrak{p}}\right) = 1$. D'après cette dernière égalité, $\mathfrak{p}$ se décompose dans C en l idéaux premiers (théorème 149). $\mathfrak{P}$ étant l'un d'eux, l'idéal $\mathfrak{P}^m$ a évidemment, vu (157) et (158), pour caractères distinctifs les racines $l^{\text{ièmes}}$ de l'unité données $\gamma_1, \dots, \gamma_r$, et le théorème 164 est ainsi complètement démontré dans le cas considéré. Si $\mathfrak{l}$ figure dans le discriminant relatif du corps C, il faut apporter à la démonstration une modification facile à déduire par analogie de ce qui a été dit dans le cas du corps quadratique (voir § 81).

Kummer a basé ses recherches sur un certain anneau de nombres du corps $C = c(\sqrt[l]{\mu}, \zeta)$ et non sur la totalité des entiers de ce corps. La notion du genre subit alors un changement. Kummer a eu le grand mérite de découvrir et de démontrer pour cet anneau le théorème qui répond au théorème 164. [Kummer[20].] En dehors de l'anneau étudié par Kummer, il y en a encore dans C une infinité dont la théorie pourrait se développer avec autant de succès.

§ 164. — Les classes du genre principal dans un corps kummerien régulier.

Nous plaçons dans ce paragraphe et le suivant quelques conséquences importantes du théorème fondamental 164 analogues aux théorèmes développés pour le corps quadratique dans les paragraphes 71, 72 et 82.

Théorème 165. — Le nombre des genres g d'un corps kummerien régulier est égal au nombre de ses complexes invariants.

Démonstration. — t et n ayant le même sens qu'au théorème 159, si l'on considère que $g = l^{r-1}$ (théorème 164), il résulte du lemme 34 : $r - 1 \leq t - n - \frac{l-1}{2}$, et

comme, d'après le lemme 33, on doit avoir $t + n - \frac{l+1}{2} \leqq r - 1$, il en résulte

$$r - 1 = t + n - \frac{l+1}{2}.$$

Le nombre a des complexes invariants (déterminé dans la démonstration du lemme 34) est, par suite, l^{r-1}; on a donc $a = g$.

Théorème 166. — *Tout complexe du genre principal dans un corps kummerien régulier est la* $(1 - S)^{\text{ième}}$ *puissance symbolique d'un complexe de* C, *c'est-à-dire que toute classe du genre principal est le produit de la* $(1 - S)^{\text{ième}}$ *puissance symbolique d'une classe et d'une classe contenant des idéaux de* $c(\zeta)$.

Démonstration. — On a obtenu, dans la démonstration du lemme 34, l'égalité $af' = gf$; a est le nombre des complexes invariants, f' celui des complexes égaux à des $(1 - S)^{\text{ièmes}}$ puissances symboliques de complexes, g est le nombre des genres, f celui des complexes du genre principal. Comme, d'après le théorème 165, $a = g$, on a $f' = f$, ce qui démontre que tout complexe du genre principal est la $(1 - S)^{\text{ième}}$ puissance symbolique d'un complexe.

§ 165. — Sur les normes relatives des nombres d'un corps kummerien régulier.

Théorème 167. — ν, μ *étant deux entiers du corps circulaire régulier* $c(\zeta)$, μ *non égal à la* $l^{\text{ième}}$ *puissance d'un nombre de* $c(\zeta)$, *et vérifiant, pour tout ideal premier* $\mathfrak{w}$ *de* $c(\zeta)$, *la condition*

$$\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1,$$

le nombre ν *est toujours égal à la norme relative d'un entier ou d'une fraction* A *du corps kummerien* $C = c(\sqrt[l]{\mu}, \zeta)$.

Démonstration. — Démontrons d'abord ce théorème dans le cas où ν est une unité de $c(\zeta)$. Donnons encore à t et à n le même sens qu'au théorème 159; dans la démonstration du théorème 165, on a montré que $r - 1 = t + n - \frac{l+1}{2}$, c'est-à-dire que $n = \frac{l-1}{2} - t + r$. Considérons, d'autre part, les $r^* = t - r$ unités $\varepsilon_1, \ldots, \varepsilon_{r^*}$ définies au paragraphe 149. Vu les égalités (140), un produit de puissances de ces r^* unités ne peut être la $l^{\text{ème}}$ puissance d'une unité de $c(\zeta)$ que si tous les exposants sont divisibles par l. On peut donc, la totalité des unités de $c(\zeta)$ formant une famille de degré $\frac{l-1}{2}$, déterminer $\frac{l-1}{2} - r^*$ autres unités : $\varepsilon_{r^*+1}, \varepsilon_{r^*+2}, \ldots, \varepsilon_{\frac{l-1}{2}}$ de $c(\zeta)$, telles

que toute unité ξ de $c(\zeta)$ puisse se représenter par

$$\xi = \varepsilon_1^{x_1}\,\varepsilon_2^{x_2}\dots\varepsilon_{\frac{l-1}{2}}^{x_{\frac{l-1}{2}}}\,\varepsilon^{l},$$

$x_1, \dots, x_{\frac{l-1}{2}}$ étant des exposants entiers rationnels et ε une unité appropriée de $c(\zeta)$. En posant alors

$$\left(\frac{\varepsilon_u,\nu}{\mathfrak{l}_{t-i+1}}\right) = \zeta^{e_{ui}}$$
$$\left(u = 1, 2, \dots, \frac{l-1}{2};\ i = 1, 2, \dots, r^*\right)$$

les r^* égalités

(160) $$\left(\frac{\xi,\nu}{\mathfrak{l}_t}\right) = 1,\quad \left(\frac{\xi,\nu}{\mathfrak{l}_{t-1}}\right) = 1,\quad \dots,\quad \left(\frac{\xi,\nu}{\mathfrak{l}_{t-r^*+1}}\right) = 1$$

donnent les r^* congruences linéaires en $x_1, x_2, \dots, x_{\frac{l-1}{2}}$

(161) $$\left.\begin{aligned} &e_{11}x_1 + e_{21}x_2 + \dots + e_{\frac{l-1}{2},1}\,x_{\frac{l-1}{2}} \equiv 0,\\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\\ &e_{1r^*}x_1 + e_{2r^*}x_2 + \dots + e_{\frac{l-1}{2},r^*}\,x_{\frac{l-1}{2}} \equiv 0, \end{aligned}\right\}\ (\mathrm{mod}\ l).$$

A cause de (140), nous avons

$$\left.\begin{array}{llllll} e_{11}\equiv 1, & e_{21}\equiv 0, & e_{31}\equiv 0, & \dots, & e_{r^*1} & \equiv 0,\\ & e_{22}\equiv 1, & e_{32}\equiv 0, & \dots, & e_{r^*2} & \equiv 0,\\ & & e_{33}\equiv 1, & \dots, & e_{r^*3} & \equiv 0,\\ & & \dots & \dots & \dots & \dots\\ & & & & e_{r^*r^*} & \equiv 1, \end{array}\right\}\ (\mathrm{mod}\ l),$$

et par suite les r^* congruences linéaires (161) sont indépendantes; il en résulte que toutes les unités ξ remplissant les conditions (160) forment une famille d'unités de degré $\frac{l-1}{2} - r^* = \frac{l-1}{2} - t + r$.

Nous avons établi, au début de cette démonstration, que le degré n de la famille de toutes les unités de $c(\zeta)$, normes relatives d'unités ou de fractions de C, a la même valeur. Comme, de plus, toute unité de $c(\zeta)$, norme relative d'une unité ou d'une fraction de C, est évidemment résidu de normes de C, mod $\mathfrak{l}$ et doit par suite (théorème 151) vérifier aussi les égalités (160), toute unité de la première famille appartient aussi à la seconde; ces deux familles ayant même degré sont donc identiques. Or, l'unité donnée ν satisfait par hypothèse aux conditions (160) et appartient, par suite, à la seconde famille; ν est donc aussi contenue dans la première, c'est-à-dire que ν est norme relative d'une unité ou d'une fraction de C.

Soit maintenant ν un entier quelconque de $c(\zeta)$, vérifiant les conditions du théorème 167; considérons les facteurs idéaux premiers de ν dans $c(\zeta)$. Posons $\lambda = 1 - \zeta$

et $\mathfrak{l} = (\lambda)$. Si l'idéal premier $\mathfrak{l}$ entre dans ν, mais avec un exposant b non divisible par l, et qu'il n'entre pas dans le discriminant relatif du corps C, on a, d'après la fin du paragraphe 133,

$$\left(\frac{\nu,\,\mu}{\mathfrak{l}}\right) = \left(\frac{\lambda^b,\,\mu}{\mathfrak{l}}\right) = \left(\frac{\mu}{\mathfrak{l}}\right)^{-b},$$

et, vu l'égalité qu'on en tire, $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$, $\mathfrak{l}$ est (théorème 149) décomposable dans C en l facteurs premiers. Si $\mathfrak{L}$ est l'un d'eux, on a : $\mathfrak{l} = N_c(\mathfrak{L})$.

Soit ensuite $\mathfrak{p}$ un idéal premier de $c(\zeta)$ autre que $\mathfrak{l}$, et entrant dans ν avec un exposant b non divisible par l; au contraire, supposons son exposant a dans μ divisible par l; on a alors par définition

$$\left(\frac{\nu,\,\mu}{\mathfrak{p}}\right) = \left(\frac{\mu^b}{\mathfrak{p}}\right)^{-1},$$

et il en résulte, vu l'hypothèse du théorème 167, $\left\{\frac{\mu}{\mathfrak{p}}\right\} = 1$; donc (théorème 149) $\mathfrak{p}$ est aussi dans C le produit de l idéaux premiers. $\mathfrak{P}$ étant l'un d'eux, on a $\mathfrak{p} = N_c(\mathfrak{P})$.

Enfin, les idéaux premiers de $c(\zeta)$ facteurs du discriminant relatif de C sont toujours des puissances $l^{\text{ièmes}}$ d'idéaux premiers de C et sont par suite aussi normes relatives d'idéaux de C. De tout cela résulte que ν doit être norme relative d'un idéal $\mathfrak{H}$ de C : $\nu = N_c(\mathfrak{H})$.

De plus, vu l'hypothèse du théorème 167, $\mathfrak{H}$ appartient au genre principal de C et nous pouvons par suite poser, d'après le théorème 166,

$$\mathfrak{H} \sim \mathfrak{j}\,\mathfrak{J}^{1-S},$$

$\mathfrak{j}$ étant un idéal de $c(\zeta)$ et $\mathfrak{J}$ un idéal de C. Si h est le nombre des classes d'idéaux de $c(\zeta)$, on a $\mathfrak{j}^h \sim 1$, et par suite $\mathsf{A} = \left(\frac{\mathfrak{H}}{\mathfrak{J}^{1-S}}\right)^h$ doit être un nombre entier ou fractionnaire de C ; sa norme relative $N_c(\mathsf{A})$ est évidemment égale à $\varepsilon\nu^h$, ε étant une unité de $c(\zeta)$. De la dernière égalité résulte, d'après le théorème 151, que l'on a, pour tout idéal premier $\mathfrak{w}$ de $c(\zeta)$, $\left(\frac{\varepsilon\nu^h,\,\mu}{\mathfrak{w}}\right) = 1$, et par suite aussi $\left(\frac{\varepsilon,\,\mu}{\mathfrak{w}}\right) = 1$. Or, on a montré, dans la première partie de la démonstration, que dans ces conditions ε doit être norme relative d'un nombre de C ; posons $\varepsilon = N_c(\mathsf{H})$, H étant un nombre de C. b et e étant alors des entiers rationnels tels que l'on ait $bh + el = 1$, on a

$$\nu = N_c(\mathsf{A}^b \mathsf{H}^{-b} \nu^e),$$

et la démonstration du théorème 167 est ainsi complète.

Dans cette démonstration nous pouvons, dans les deux cas, restreindre l'application du théorème 151 au cas de $\mathfrak{w} \neq \mathfrak{l}$, car d'après le théorème 163 les conclusions subsistent, même pour $\mathfrak{w} = \mathfrak{l}$.

On est ainsi parvenu à étendre aux corps kummeriens réguliers toutes les propriétés déjà établies et démontrées par Gauss pour les corps quadratiques.

CHAPITRE XXXV.

Nouvelle méthode pour la théorie d'un corps kummerien régulier.

§ 166. — Propriétés essentielles des unités d'un corps circulaire régulier.

Nous avons vu quel rôle important joue le symbole $\left\{\frac{\nu,\,\mu}{\mathfrak{l}}\right\}$ dans la théorie des corps kummeriens. Pour la définition de ce symbole (paragraphe 131) et la recherche de ses propriétés, du paragraphe 131 au paragraphe 133 nous avons, comme Kummer, introduit les dérivées de logarithmes des polynômes $\omega(x)$, adjoints à un nombre $\omega \equiv 1$, mod $\mathfrak{l}$. Les calculs des paragraphes 131 *bis* à 133 pour le symbole $\left\{\frac{\nu,\,\mu}{\mathfrak{l}}\right\}$ dans les corps kummeriens correspondent d'ailleurs aux considérations du paragraphe 64 pour le symbole $\left(\frac{n,\,m}{2}\right)$ du corps quadratique. Quoique nous soyons déjà parvenus à réduire à de moindres proportions les calculs employés par Kummer, il me paraît cependant nécessaire, surtout en vue du développement futur de la théorie, de chercher s'il n'est pas possible d'édifier la théorie des corps kummeriens sans ces calculs. J'indique brièvement dans ce chapitre la marche à suivre.

D'abord on peut établir aisément sans calcul et sans les nombres de Bernoulli les propriétés essentielles ci-après des unités du corps circulaire régulier $c(\zeta)$. Rappelons-nous, pour le théorème 156, la dernière démonstration indiquée au paragraphe 141.

Nous pouvons alors déduire, du théorème 156, le théorème 155 de la manière suivante. Nous entendons par $\varepsilon_1, \ldots, \varepsilon_{l^*}$ un système quelconque de l^* unités réelles de $c(\zeta)$; nous déterminons alors des exposants positifs $e_1, \ldots, e_{l^*}$ et des entiers rationnels $a_1, \ldots, a_{l^*}, b_1, \ldots, b_{l^*}$, vérifiant les congruences

$$\varepsilon_1 \equiv a_1 + b_1 \lambda^{e_1}, \qquad (\mathfrak{l}^{e_1+1}),$$

$$\cdots\cdots\cdots\cdots$$

$$\varepsilon_{l^*} \equiv a_{l^*} + b_{l^*} \lambda^{e_{l^*}}, \qquad (\mathfrak{l}^{e_{l^*}+1}).$$

Nous supposons que e_1 ait la valeur minima parmi les exposants e. Nous pouvons alors, on le voit aisément, multiplier les $l^* - 1$ unités $\varepsilon_2, \ldots, \varepsilon'_{l^*}$ par des puissances de ε_1, telles que ces $l^* - 1$ produits $\varepsilon'_2, \ldots, \varepsilon'_{l^*}$ vérifient les congruences

$$\varepsilon'_2 = \varepsilon_2 \varepsilon_1^{f_2} \equiv a'_2 + b'_2 \lambda^{e'_2}, \qquad (\mathfrak{l}^{e'_2+1}),$$

$$\cdots\cdots\cdots\cdots$$

$$\varepsilon'_{l^*} = \varepsilon_{l^*} \varepsilon_1^{f_{l^*}} \equiv a'_{l^*} + b'_{l^*} \lambda^{e'_{l^*}}, \qquad (\mathfrak{l}^{e'_{l^*}+1})$$

les a' et les b' étant des entiers rationnels premiers à l, et les exposants $e'_2, \ldots, e'_{l^*}$ étant tous plus grands que e_1. Les unités $\varepsilon_1, \varepsilon'_2, \varepsilon'_3, \ldots, \varepsilon'_{l^*}$ forment encore un système d'unités fondamentales dans $c(\zeta)$. Soit e'_2 le moindre des e'; il est encore possible de multiplier les unités $\varepsilon'_3, \ldots, \varepsilon'_{l^*}$ par des puissances de ε'_2, de manière que les l^*-2 produits obtenus $\varepsilon''_3, \ldots, \varepsilon''_{l^*}$ vérifient les congruences

$$\varepsilon''_3 = \varepsilon'_3 \varepsilon'^{f_3}_2 \equiv a''_3 + b''_3 \lambda^{e''_3}, \qquad (\mathfrak{l}^{e''_3+1}),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\varepsilon''_{l^*} = \varepsilon'_{l^*} \varepsilon'^{f_{l^*}}_2 \equiv a''_{l^*} + b''_{l^*} \lambda^{e''_{l^*}}, \qquad (\mathfrak{l}^{e''_{l^*}+1}),$$

les a'' et b'' premiers à l et les e'' tous plus grands que e'_2.

Les unités $\varepsilon_1, \varepsilon'_2, \varepsilon''_3, \varepsilon''_4, \ldots, \varepsilon''_{l^*}$ forment encore un système d'unités fondamentales de $c(\zeta)$. En poursuivant ainsi, nous arrivons à un système d'unités fondamentales de $c(\zeta)$, $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon^{(l^*-1)}_{l^*}$ vérifiant les congruences

$$\begin{aligned}
\varepsilon_1 &\equiv a_1 + b_1 \lambda^{e_1}, & (\mathfrak{l}^{e_1+1}),\\
\varepsilon'_2 &\equiv a'_2 + b'_2 \lambda^{e'_2}, & (\mathfrak{l}^{e'_2+1}),\\
\varepsilon''_3 &\equiv a''_3 + b''_3 \lambda^{e''_3}, & (\mathfrak{l}^{e''_3+1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots & \\
\varepsilon^{(l^*-1)}_{l^*} &\equiv a^{(l^*-1)}_{l^*} + b^{(l^*-1)}_{l^*} \lambda^{e^{(l^*-1)}_{l^*}}, & (\mathfrak{l}^{e^{(l^*-1)}_{l^*}+1}),
\end{aligned}$$

les a et les b étant premiers à l et les exposants $e_1, \ldots, e^{(l^*-1)}_{l^*}$ vérifiant les inégalités

(162) $$e_1 < e'_2 < e''_3 < \ldots < e^{(l^*-1)}_{l^*}.$$

Comme les unités considérées sont toutes réelles, tous les exposants $e_1, e'_2, \ldots$ sont pairs. Or, si on avait

$$e^{(l^*-1)}_{l^*} \geqq l-1,$$

$\varepsilon^{(l^*-1)}_{l^*}$ serait, d'après le théorème 156, la $l^{\text{ième}}$ puissance d'une unité η de $c(\zeta)$. En exprimant alors η au moyen des unités $\zeta, \varepsilon_1, \varepsilon'_2, \ldots, \varepsilon^{(l^*-1)}_{l^*}$ sous la forme

$$\eta = \zeta^u \varepsilon_1^{u_1} \varepsilon'^{u_2}_2 \ldots (\varepsilon^{(l^*-1)}_{l^*})^{u_{l^*}},$$

les u étant des exposants entiers rationnels, et en élevant cette égalité à la $l^{\text{ième}}$ puissance, nous obtenons une relation entre les l^* unités $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon^{(l^*-1)}_{l^*}$ avec des exposants non tous nuls; ceci est contraire au fait que $\varepsilon_1, \varepsilon'_2, \ldots, \varepsilon^{(l^*-1)}_{l^*}$ forment un système d'unités fondamentales de $c(\zeta)$. Par suite, on a

$$\varepsilon^{(l^*-1)}_{l^*} < l-1.$$

Il en résulte, vu les inégalités (162), que l'on a nécessairement

$$e_1 = 2, \quad e'_2 = 4, \quad e''_3 = 6, \quad \ldots, \quad e^{(l^*-1)}_{l^*} = l-3,$$

et on en conclut immédiatement l'existence d'unités $\varepsilon_1, \ldots, \varepsilon_{l^*}$ ayant les propriétés indiquées au théorème 155.

Le théorème 157 résulte, comme au paragraphe 142, du théorème 155.

§ 167. — Démonstration d'une propriété des nombres primaires d'idéaux premiers de seconde espèce.

Nous nous basons sur la définition du symbole $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ donnée paragraphe 131, mais nous nous passons provisoirement du symbole $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$; nous n'utilisons par suite les théorèmes 150, 151 que pour $\mathfrak{w} = \mathfrak{l}$. Les théorèmes 158 et 159 s'établissent alors immédiatement comme on l'a montré, si l'on fait l'hypothèse restrictive que le discriminant relatif de $c(\sqrt[l]{\mu}, \zeta)$ par rapport à $c(\zeta)$ est premier à $\mathfrak{l}$. Avec cette restriction, nous arrivons, sans employer le symbole $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$, à la notion de caractère d'un idéal de $c(\sqrt[l]{\mu}, \zeta)$, à la division des classes d'idéaux d'un corps kummerien en genres, ainsi qu'aux lemmes 33, 34, 35, et nous démontrons ensuite le lemme suivant :

Lemme 43. — Tout nombre primaire $\varkappa$ d'un idéal premier $\mathfrak{q}$ de seconde espèce est congru mod $\mathfrak{l}^l$ à la $l^{\text{ième}}$ puissance d'un entier de $c(\zeta)$.

Démonstration. — Soient $\varepsilon_1, \ldots, \varepsilon_{l^*}$, les $l^* = \frac{l-3}{2}$ unités fondamentales du corps $c(\zeta)$ définies au paragraphe 166 et désignées alors par $\varepsilon_1, \ldots, \varepsilon_{l^*}^{(l^*-1)}$; soient ensuite $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$ des idéaux premiers de $c(\zeta)$ autres que $\mathfrak{l}$, tels que l'on ait

$$(163)\quad \begin{cases} \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^*, & \left\{\frac{\varepsilon_1}{\mathfrak{p}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}}\right\} = 1, \\ \left\{\frac{\zeta}{\mathfrak{p}_1}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_1}\right\} = \zeta_1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_1}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_1}\right\} = 1, \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \left\{\frac{\zeta}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_1}{\mathfrak{p}_{l^*}}\right\} = 1, & \left\{\frac{\varepsilon_2}{\mathfrak{p}_{l^*}}\right\} = 1, & \ldots, & \left\{\frac{\varepsilon_{l^*}}{\mathfrak{p}_{l^*}}\right\} = \zeta_{l^*}, \end{cases}$$

$\zeta^*, \zeta_1, \ldots, \zeta_{l^*}$ étant des racines $l^{\text{ièmes}}$ de l'unité quelconque autres que 1. L'existence de tels idéaux résulte du théorème 152 ; en nous reportant à la démonstration de ce théorème, nous voyons que non seulement le nombre, mais encore la somme des inverses des normes de tous les idéaux premiers $\mathfrak{r}$ y étaient infinies, et ceci nous permet, comme le montrent les considérations faites en démontrant le théorème 83, de supposer du premier degré dans le cas actuel tous les idéaux premiers $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$. Nous pouvons aussi supposer tous différents les nombres premiers rationnels divisibles par $\mathfrak{p}, \mathfrak{p}_1, \ldots, \mathfrak{p}_{l^*}$. Soient $\pi, \pi_1, \ldots, \pi_{l^*}$ des nombres primaires de ces idéaux.

Occupons-nous maintenant du cas où il existerait $l^* + 1$ exposants entiers

$u, u_1, \ldots, u_l$, non tous divisibles par l, tels que l'expression $\alpha = \pi^u \pi_1^{u_1} \ldots \pi_l^{u_l}$ soit congrue mod $\mathfrak{l}^l$ à la $l^{\text{ième}}$ puissance d'un entier de $c(\zeta)$. D'après le théorème 148, le discriminant relatif du corps kummerien $c(\sqrt[l]{\alpha}, \zeta)$ renferme alors comme facteurs un certain nombre t des idéaux premiers $\mathfrak{p}, \ldots, \mathfrak{p}_l$, mais non l'idéal $\mathfrak{l}$. D'autre part, il résulte de (163) et du théorème 151 que le degré m de la famille des unités de $c(\zeta)$, normes relatives d'unités de $c(\sqrt[l]{\alpha}, \zeta)$, est au plus $\frac{l-1}{2} = t$; on aurait alors pour le corps kummerien $c(\sqrt[l]{\alpha}, \zeta)$

$$m \leqq \frac{l-1}{2} - t, \quad \text{c.-à-d.} \quad t + m - \frac{l+1}{2} < 0,$$

ce qui est impossible d'après le théorème 158. Le cas envisagé est donc impossible.

Soit $\varkappa$ un nombre primaire de l'idéal premier $\mathfrak{q}$. Nous déduisons de la démonstration du théorème 157 qu'il existe exactement $\frac{(l-1)l^{l-3}}{l^e}$, nombres primaires de $c(\zeta)$ incongrus, mod $\mathfrak{l}^{l-1}$, et, par suite, $(l-1)l^{e+1}$ incongrus, mod $\mathfrak{l}^l$; d'autre part, la $l^{\text{ième}}$ puissance de tout entier de $c(\zeta)$ premier à $\mathfrak{l}$ est congrue mod $\mathfrak{l}^l$ à l'un des $l-1$ nombres $1, 2, \ldots, l-1$. De ce qui précède résulte alors qu'il est toujours possible de déterminer les exposants $u, u_1, \ldots, u_{l^*}$ de manière à ce que l'expression $\mu = \pi^u \pi_1^{u_1} \ldots \pi_l^{u_l} \varkappa$ soit congrue, mod $\mathfrak{l}^l$, à la $l^{\text{ième}}$ puissance d'un entier de $c(\zeta)$; $u, u_1, \ldots, u_{l^*}$ étant ainsi déterminés, posons $\alpha = \varkappa^u \ldots \varkappa_{l^*}^{u_{l^*}}$, de sorte que $\mu = \alpha\varkappa$, et occupons-nous maintenant du cas où un certain nombre *positif* a des exposants u, $u_1, \ldots, u_{l^*}$ sont premiers à l, les $\frac{l-1}{2} - a$ autres étant divisibles par l. On aurait alors, vu (163), pour le corps kummerien $c(\sqrt[l]{\mu}, \zeta)$, avec les notations du paragraphe 149, $t = a + 1$, $r^* = a$, $r = t - r^* = 1$, et, par suite, d'après le lemme 35, toutes les classes d'idéaux de ce corps sont du genre principal. D'où le résultat suivant : $\mathfrak{r}$ étant un idéal premier quelconque de $c(\zeta)$, tel que l'on ait $\left\{\frac{\mu}{\mathfrak{r}}\right\} = 1$, et ρ désignant un nombre primaire de $\mathfrak{r}$, le nombre $\xi\rho$ aura, avec un choix convenable de l'unité ξ, tous ses caractères égaux à 1 dans le corps $c(\sqrt[l]{\mu}, \zeta)$; on a donc en particulier

$$\left\{\frac{\xi\rho, \mu}{\mathfrak{q}}\right\} = \left\{\frac{\xi\rho}{\mathfrak{q}}\right\} = 1,$$

et comme $\mathfrak{q}$ est idéal de deuxième espèce, on a aussi $\left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$.

Désignons maintenant les idéaux premiers conjugués de $\mathfrak{q}$ et autres que $\mathfrak{q}$ par $\mathfrak{q}', \mathfrak{q}'', \ldots$, et les substitutions du groupe de $c(\zeta)$ changeant $\mathfrak{q}$ en $\mathfrak{q}', \mathfrak{q}'', \ldots$ par s', $s'', \ldots$; h et h^* ayant alors la signification du paragraphe 149 et q étant le nombre premier divisible par $\mathfrak{q}$, on a, vu la remarque à la fin du théorème 157,

$$\varkappa . (s'\varkappa) . (s''\varkappa) \ldots = \varepsilon' q^{hh^*}.$$

ε étant une unité de $c(\zeta)$. Vu notre hypothèse sur les exposants $u, u_1, \ldots, u_l$, les idéaux $\mathfrak{p}, \ldots, \mathfrak{p}_{l^*}$ étant du premier degré et les nombres premiers qu'ils contiennent étant distincts, nous pouvons conclure du théorème 152 qu'il existe dans $c(\zeta)$ un idéal premier $\mathfrak{r}$ tel que l'on ait

$$(164)\qquad \begin{cases} \left\{\dfrac{\alpha}{\mathfrak{r}}\right\} = \zeta^{*-1}, & \left\{\dfrac{\varkappa}{\mathfrak{r}}\right\} = \zeta^{*}, \\[2ex] \left\{\dfrac{s'\varkappa}{\mathfrak{r}}\right\} = 1, & \left\{\dfrac{s'\varkappa}{\mathfrak{r}}\right\} = 1, \\[2ex] \left\{\dfrac{s''\varkappa}{\mathfrak{r}}\right\} = 1, & \left\{\dfrac{s''\varkappa}{\mathfrak{r}}\right\} = 1, \\ \ldots\ldots & \ldots\ldots \end{cases}$$

ζ^* étant une racine $l^{\text{ième}}$ de l'unité autre que 1. Ces égalités (164) donnent de suite

$$(165)\qquad \left\{\frac{\mu}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{s'\mu}{\mathfrak{r}}\right\} = 1, \quad \left\{\frac{s''\mu}{\mathfrak{r}}\right\} = 1, \quad \ldots,$$

$$(166)\qquad \left\{\frac{\varkappa.s'\varkappa.s''\varkappa\ldots}{\mathfrak{r}}\right\} = \left\{\frac{q}{\mathfrak{r}}\right\} = \zeta^{*}.$$

La première égalité (165) donne, d'après ce qui précède, $\left\{\dfrac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$, et les suivantes donnent de même $\left\{\dfrac{\mathfrak{r}}{\mathfrak{q}'}\right\} = 1$, $\left\{\dfrac{\mathfrak{r}}{\mathfrak{q}''}\right\} = 1, \ldots$; d'où, en faisant le produit, $\left\{\dfrac{\mathfrak{r}}{q}\right\} = 1$, ce qui est incompatible avec (166), vu le théorème 140.

Notre point de départ est donc faux et tous les exposants $u, u_1, \ldots, u_l$ doivent être divisibles par l; α est donc la $l^{\text{ième}}$ puissance d'un nombre de $c(\zeta)$; on en déduit que $\varkappa$ est congru à la $l^{\text{ième}}$ puissance d'un entier de $c(\zeta)$, mod $\mathfrak{l}^l$, ce qui démontre le lemme 43.

§ 168. — Démonstration de la loi de réciprocité pour les cas où l'un des deux idéaux premiers est de seconde espèce.

Lemme 44. — Soit $\mathfrak{q}$ un idéal premier de seconde espèce et $\mathfrak{r}$ un idéal premier de première ou de seconde espèce de $c(\zeta)$; alors si $\left\{\dfrac{\mathfrak{q}}{\mathfrak{r}}\right\} = 1$, on a aussi $\left\{\dfrac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1$.

Démonstration. — Soient $\varkappa$, ρ des nombres primaires de $\mathfrak{q}$, $\mathfrak{r}$. D'après le lemme 43, le discriminant relatif du corps $c(\sqrt[l]{\varkappa}, \zeta)$ ne possède (théorème 148) qu'un seul facteur premier $\mathfrak{q}$ et tous les idéaux de ce corps (lemme 35) appartiennent alors au genre principal. Comme on a $\left\{\dfrac{\mathfrak{q}}{\mathfrak{r}}\right\} = 1$, $\mathfrak{r}$ est dans le corps $c(\sqrt[l]{\varkappa}, \zeta)$ le produit de

l idéaux premiers; nous avons pour le caractère d'un de ces l idéaux premiers la valeur

$$\left\{\frac{\rho,\ \varkappa}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = 1,$$

ce qui démontre le lemme.

Lemme 45. — $\mathfrak{q}$, $\bar{\mathfrak{q}}$ étant deux idéaux premiers quelconques de seconde espèce de $c(\zeta)$, on a toujours $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\} = \left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{q}}\right\}$.

Démonstration. — $\left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}$ est $\neq 1$ (le cas contraire venant d'être démontré). Soient $\varkappa$, $\bar{\varkappa}$ des nombres primaires de $\mathfrak{q}$, $\bar{\mathfrak{q}}$; $\mathfrak{q}'$, $\mathfrak{q}''$, ... les idéaux premiers conjugués de $\mathfrak{q}$ et distincts de ce dernier; $\varkappa'$, $\varkappa''$, ... les nombres primaires correspondants conjugués de $\varkappa$. Mêmes notations avec $^{-}$ pour $\bar{\mathfrak{q}}$ et $\bar{\varkappa}$. Soit enfin q le nombre premier divisible par $\mathfrak{q}$; on a alors $\varkappa\varkappa'\varkappa''\ldots = \varepsilon' q^{hh^*}$, ε étant une unité de $c(\zeta)$. D'après le théorème 152, il existe un idéal $\mathfrak{r}$ pour lequel on a

(167) $$\left\{\frac{\varkappa}{\mathfrak{r}}\right\} = \zeta^*,\quad \left\{\frac{\varkappa'}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varkappa''}{\mathfrak{r}}\right\} = 1,\quad \ldots,$$

(168) $$\left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\} = \zeta^{**},\quad \left\{\frac{\bar{\varkappa}'}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\bar{\varkappa}''}{\mathfrak{r}}\right\} = 1,\quad \ldots,$$

(169) $$\left\{\frac{\zeta}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varepsilon_1}{\mathfrak{r}}\right\} = 1,\quad \left\{\frac{\varepsilon_2}{\mathfrak{r}}\right\} = 1,\quad \ldots,\quad \left\{\frac{\varepsilon_l}{\mathfrak{r}}\right\} = 1,$$

ζ^* étant une racine $l^{\text{ième}}$ de l'unité autre que 1 de $c(\zeta)$ et où $\varepsilon_1, \ldots, \varepsilon_l$ désignent les l^* unités désignées par $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{l^*}^{(l^*-1)}$ au paragraphe 166. De (167) on tire

$$\left\{\frac{\varkappa\varkappa'\varkappa''\ldots}{\mathfrak{r}}\right\} = \left\{\frac{q}{\mathfrak{r}}\right\} = \zeta^*,$$

et par suite aussi, ρ étant un nombre primaire de $\mathfrak{r}$ (voir théorème 140),

(170) $$\left\{\frac{\rho}{q}\right\} = \left\{\frac{\rho}{\mathfrak{q}}\right\}\left\{\frac{\rho}{\mathfrak{q}'}\right\}\left\{\frac{\rho}{\mathfrak{q}''}\right\}\ldots = \zeta^*.$$

D'autre part, on a, vu (167) et le lemme 44,

$$\left\{\frac{\rho}{\mathfrak{q}'}\right\} = 1,\quad \left\{\frac{\rho}{\mathfrak{q}''}\right\} = 1,\ \ldots,$$

et par suite on tire de (170) : $\left\{\frac{\rho}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} = \zeta^*$.

On a donc

(171) $$\left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\} \neq 1.$$

On tire de même de (168) la relation

$$(172) \qquad \left\{\frac{\bar{\mathfrak{q}}}{\mathfrak{r}}\right\} = \left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\} \neq 1.$$

Déterminons maintenant la puissance ρ^e de ρ de façon que l'on ait $\left\{\frac{\varkappa\rho^e}{\mathfrak{q}}\right\} = 1$, et considérons le corps kummerien $c\left(\sqrt[l]{\varkappa\rho^e}, \zeta\right)$. Comme $\mathfrak{q}$ par hypothèse et $\mathfrak{r}$ à cause de (169) sont idéaux de seconde espèce, il résulte du lemme 43 que le discriminant relatif de ce corps ne contient que les deux idéaux premiers $\mathfrak{q}$ et $\mathfrak{r}$. Le corps $c\left(\sqrt[l]{\varkappa\rho^e}, \zeta\right)$ contient alors au plus l genres (lemme 35). L'idéal premier $\mathfrak{r}$ est la $l^{\text{ième}}$ puissance d'un idéal premier $\mathfrak{R}$ de $c\left(\sqrt[l]{\varkappa\rho^e}, \zeta\right)$. Les deux caractères de $\mathfrak{R}$ dans ce corps sont

$$\left\{\frac{\rho, \varkappa\rho^e}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{r}}{\mathfrak{q}}\right\}, \qquad \left\{\frac{\rho, \varkappa\rho^e}{\mathfrak{r}}\right\} = \left\{\frac{\varkappa}{\mathfrak{r}}\right\}^{-1} = \left\{\frac{\mathfrak{q}}{\mathfrak{r}}\right\}^{-1}.$$

et on en déduit les caractères de $\mathfrak{R}^2, \mathfrak{R}^3, \ldots, \mathfrak{R}^l$.

Les l idéaux $\mathfrak{R}, \mathfrak{R}^2, \ldots, \mathfrak{R}^l$ déterminent, vu (171), l genres différents et le produit des deux caractères de chacun d'eux est égal à 1 d'après la même formule. Ce dernier résultat est par suite vrai pour tout idéal de $c\left(\sqrt[l]{\varkappa\rho^e}, \zeta\right)$. Comme on a $\left\{\frac{\varkappa\rho^e}{\mathfrak{q}}\right\} = 1$, $\bar{\mathfrak{q}}$ est décomposable dans $c\left(\sqrt[l]{\varkappa\rho^e}, \zeta\right)$; les caractères d'un facteur premier de $\bar{\mathfrak{q}}$ sont :

$$\left\{\frac{\bar{\varkappa}, \varkappa\rho^e}{\mathfrak{q}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\}, \qquad \left\{\frac{\bar{\varkappa}, \varkappa\rho^e}{\mathfrak{r}}\right\} = \left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e,$$

et par suite on a

$$\left\{\frac{\bar{\varkappa}}{\mathfrak{q}}\right\}\left\{\frac{\bar{\varkappa}}{\mathfrak{r}}\right\}^e = 1.$$

Comme on doit avoir, d'autre part,

$$\left\{\frac{\varkappa\rho^e}{\bar{\mathfrak{q}}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}\left\{\frac{\mathfrak{r}}{\bar{\mathfrak{q}}}\right\}^e = 1,$$

on en déduit, d'après 172,

$$\left\{\frac{\mathfrak{q}}{\mathfrak{q}}\right\} = \left\{\frac{\mathfrak{q}}{\bar{\mathfrak{q}}}\right\}.$$

Lemme 46. — Soit $\mathfrak{p}$ un idéal premier de première espèce et $\mathfrak{q}$ un idéal premier de seconde espèce de $c(\zeta)$; si l'on a $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} = 1$, on a aussi $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} = 1$.

Démonstration. — Soient π, ζ des nombres primaires de $\mathfrak{p}$, $\mathfrak{q}$. Supposons que l'on ait $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} \neq 1$. Il existe (théorème 152) un idéal premier $\mathfrak{r}$, différent de $\mathfrak{p}$ et de $\mathfrak{q}$, pour

lequel on a

(173) $$\left(\frac{\pi}{\mathfrak{r}}\right) \neq 1, \quad \left(\frac{\varkappa}{\mathfrak{r}}\right) \neq 1,$$

(174) $$\left(\frac{\zeta}{\mathfrak{r}}\right) = 1, \quad \left(\frac{\varepsilon_1}{\mathfrak{r}}\right) = 1, \quad \ldots, \quad \left(\frac{\varepsilon_l}{\mathfrak{r}}\right) = 1,$$

$\varepsilon_1, \ldots, \varepsilon_l$ étant les unités $\varepsilon_1, \varepsilon_2', \ldots$ du paragraphe 166.

A cause de (174), $\mathfrak{r}$ est idéal premier de seconde espèce; ρ étant un nombre primaire de $\mathfrak{r}$, on a $\left(\frac{\rho}{\mathfrak{p}}\right) \neq 1$, car on déduirait de $\left(\frac{\rho}{\mathfrak{p}}\right) = 1$, à cause du lemme 44, $\left(\frac{\pi}{\mathfrak{r}}\right) = 1$, contrairement à (173). Nous pouvons alors déterminer une puissance ρ^e de ρ telle que l'on ait $\left(\frac{\varkappa\rho^e}{\mathfrak{p}}\right) = 1$. $\mathfrak{r}$, $\mathfrak{q}$ étant idéaux premiers de seconde espèce, il résulte du lemme 43 et du théorème 148 que le discriminant relatif du corps $c(\sqrt[l]{\varkappa\rho^e}, \zeta)$ ne contient que les deux idéaux premiers $\mathfrak{q}$, $\mathfrak{r}$. Or, on a d'après (173) $\left(\frac{\varkappa}{\mathfrak{r}}\right) \neq 1$, et d'après le lemme 45

$$\left(\frac{\varkappa}{\mathfrak{r}}\right) = \left(\frac{\mathfrak{q}}{\mathfrak{r}}\right) = \left(\frac{\mathfrak{r}}{\mathfrak{q}}\right),$$

et il en résulte, comme dans la démonstration du lemme 45, que le produit des deux caractères de tout idéal de $c(\sqrt[l]{\varkappa\rho^e}, \zeta)$ est égal à 1. Vu $\left(\frac{\varkappa\rho^e}{\mathfrak{p}}\right) = 1$, $\mathfrak{p}$ est décomposable dans $c(\sqrt[l]{\varkappa\rho^e}, \zeta)$; tout facteur premier de $\mathfrak{p}$ a les deux caractères

$$\left(\frac{\pi, \varkappa\rho^e}{\mathfrak{q}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right), \quad \left(\frac{\pi, \varkappa\rho^e}{\mathfrak{r}}\right) = \left(\frac{\pi}{\mathfrak{r}}\right)^e.$$

Le premier étant par hypothèse égal à 1, il faudrait que $\left(\frac{\pi}{\mathfrak{r}}\right)$ fût égal à 1, contrairement à (173).

Notre hypothèse $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) \neq 1$ est donc fausse.

Lemme 47. — $\mathfrak{q}$ étant un idéal premier de deuxième espèce et $\mathfrak{p}$ un idéal premier de première espèce, on a toujours

$$\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right) = \left(\frac{\mathfrak{p}}{\mathfrak{q}}\right).$$

Démonstration. — Nous procédons, comme dans la démonstration du lemme 45, en introduisant $\mathfrak{p}$ au lieu de $\bar{\mathfrak{q}}$ et utilisant, dans le cours de la démonstration, le lemme 46 au lieu de 44 pour établir la relation correspondante à (172).

§ 169. — Lemme sur le produit $\Pi'\left(\frac{\nu, \mu}{\mathfrak{w}}\right)$ étendu a tous les idéaux premiers $\mathfrak{w} \neq \mathfrak{l}$.

Lemme 48. — ν, μ étant deux entiers de $c(\zeta)$ premiers à $\mathfrak{l}$, μ étant de plus congru, mod $\mathfrak{l}^l$, à la $l^{\text{ème}}$ puissance d'un entier de $c(\zeta)$, on a toujours

$$\Pi'_{(\mathfrak{w})}\left(\frac{\nu, \mu}{\mathfrak{w}}\right) = 1,$$

le produit étant étendu à tous les idéaux premiers $\mathfrak{w}$ de $c(\zeta) \neq \mathfrak{l}$.

Démonstration. — Vu les hypothèses, μ peut être mis sous la forme d'un produit de nombres primaires d'idéaux premiers divisé par la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$. Si ν est en particulier égal à un nombre primaire $\varkappa$ d'un idéal premier $\mathfrak{q}$ de deuxième espèce, le lemme résulte immédiatement des lemmes 46 et 47, c'est-à dire qu'on a, avec l'hypothèse faite sur μ,

(175) $$\Pi'_{(\mathfrak{w})}\left(\frac{\varkappa, \mu}{\mathfrak{w}}\right) = 1.$$

Considérons maintenant le corps kummerien $c(\sqrt[l]{\mu}, \zeta)$. r étant le nombre des caractères distinctifs d'un genre de ce corps, il existe, d'après le lemme 35, au plus l^{r-1} genres dans ce corps. $\gamma_1, \dots, \gamma_r$ étant alors r racines $l^{\text{èmes}}$ de l'unité dont le produit soit égal à 1, nous pouvons démontrer, exactement comme dans la démonstration du théorème 164, qu'il existe toujours dans $c(\sqrt[l]{\mu}, \zeta)$ des idéaux dont les caractères sont $\gamma_1, \dots, \gamma_r$. Il n'y a qu'à ajouter aux conditions (155), (156), auxquelles doit satisfaire l'idéal désigné par $\mathfrak{p}$, les conditions supplémentaires

$$\left(\frac{\zeta}{\mathfrak{p}}\right) = 1, \quad \left(\frac{\varepsilon_1}{\mathfrak{p}}\right) = 1, \quad \dots, \quad \left(\frac{\varepsilon_{t^*}}{\mathfrak{p}}\right) = 1,$$

$\varepsilon_1, \dots, \varepsilon_{t^*}$ désignant les unités $\varepsilon_1, \dots, \varepsilon_{t^*}^{(l-1)}$ du paragraphe 166. De cette façon, on trouve de même que $\mathfrak{p}$ doit être un idéal de deuxième espèce et nous avons alors le droit, d'après les lemmes 45 et 47, d'appliquer la loi de réciprocité de la même manière qu'on l'a fait dans la démonstration du théorème 164. Au lieu du théorème 163 qu'on y a employé, nous utilisons ici la formule (175). Il en résulte en même temps qu'il y a effectivement l^{r-1} genres dans $c(\sqrt[l]{\mu}, \zeta)$ et, par suite, que le produit des r caractères doit être égal à 1 pour chacun d'eux. Appliquons maintenant ces résultats à la démonstration du lemme 48 dans le cas où ν est unité, puis dans celui où ν est nombre primaire d'un idéal premier de première espèce.

Soient encore $\varepsilon_1, \dots, \varepsilon_{t^*}$ les unités dont il vient d'être question; $\mathfrak{l}_1, \dots, \mathfrak{l}_t$ les t idéaux premiers distincts qui entrent dans le discriminant relatif de $c(\sqrt[l]{\mu}, \zeta)$, et

choisissons, comme au paragraphe 149, $\mathfrak{l}_t, \mathfrak{l}_{t-1}, \ldots, \mathfrak{l}_{r-1}$; soient $\lambda_t, \ldots, \lambda_{r-1}$ des nombres primaires correspondants et ξ une unité quelconque de $c(\zeta)$. D'après le théorème 152, il existe un idéal premier $\mathfrak{q}$ et un exposant m premier à l, tels que l'on ait

$$(176)\qquad \left\{\frac{\zeta}{\mathfrak{q}}\right\}=1,\quad \left\{\frac{\varepsilon_1}{\mathfrak{q}}\right\}=1,\quad \ldots,\quad \left\{\frac{\varepsilon_t}{\mathfrak{q}}\right\}=1,\quad \left\{\frac{\mu}{\mathfrak{q}}\right\}=1,$$

$$(177)\qquad \left\{\frac{\lambda_{r-1}}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{l}_{r-1}}\right\}^m,\quad \left\{\frac{\lambda_{r-2}}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{l}_{r-2}}\right\}^m,\quad \ldots,\quad \left\{\frac{\lambda_t}{\mathfrak{q}}\right\}=\left\{\frac{\xi}{\mathfrak{l}_t}\right\}^m.$$

Soit $\varkappa$ un nombre primaire de $\mathfrak{q}$. Vu l'égalité $\left\{\frac{\mu}{\mathfrak{q}}\right\}=1$, $\mathfrak{q}$ se décompose dans $c(\sqrt[l]{\mu}, \zeta)$, et, d'après les autres conditions (176), $\mathfrak{q}$ est idéal premier de deuxième espèce. Les r caractères d'un facteur premier de $\mathfrak{q}$ ont, comme on voit d'après (177) et les lemmes 45 et 47 que l'on a :

$$(178)\qquad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_{r-1}}\right\}=1,\quad \ldots,\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_t}\right\}=1,$$

les valeurs suivantes :

$$\left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_1}\right\},\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_2}\right\},\quad \ldots,\quad \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{l}_r}\right\}.$$

Or, d'après ce qui précède, leur produit doit être égal à 1; ceci, joint à (178) et à la dernière égalité (176), donne

$$\prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m}\varkappa,\ \mu}{\mathfrak{w}}\right\}=1,$$

le produit s'étendant à tous les idéaux premiers $\mathfrak{w}$ différents de $\mathfrak{l}$; on en tire, grâce à (175),

$$(179)\qquad \prod_{(\mathfrak{w})}{}' \left\{\frac{\xi^{-m},\ \mu}{\mathfrak{w}}\right\}=1,\quad \text{c'est-à-dire}\quad \prod_{(\mathfrak{w})}{}' \left\{\frac{\xi,\ \mu}{\mathfrak{w}}\right\}=1;$$

le lemme 48 est donc démontré quand ν est une unité quelconque de $c(\zeta)$.

Soit ensuite $\mathfrak{p}$ un idéal premier de première espèce, vérifiant la condition $\left\{\frac{\mu}{\mathfrak{p}}\right\}=1$ et, par suite, décomposable dans $c(\sqrt[l]{\mu}, \zeta)$. Les r caractères d'un facteur premier quelconque de $\mathfrak{p}$ sont :

$$\left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_1}\right\},\quad \left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_2}\right\},\quad \ldots,\quad \left\{\frac{\xi\pi,\ \mu}{\mathfrak{l}_r}\right\},$$

π désignant un nombre primaire de $\mathfrak{p}$ et ξ une unité convenable de $c(\zeta)$.

Leur produit devant être égal à 1, il en résulte encore

$$\prod_{(\mathfrak{w})}' \left\{ \frac{\xi\pi, \mu}{\mathfrak{w}} \right\} = 1,$$

et on en tire, vu (179),

$$\prod_{(\mathfrak{w})}' \left\{ \frac{\pi, \mu}{\mathfrak{w}} \right\} = 1.$$

Enfin, si $\mathfrak{p}$ est un entier premier de première espèce premier à μ, tel que l'on ait $\left\{\frac{\mu}{\mathfrak{p}}\right\} \neq 1$, on déterminera un idéal premier $\mathfrak{q}$ de seconde espèce tel que l'on ait $\left\{\frac{\mathfrak{p}}{\mathfrak{q}}\right\} \neq 1$. Alors, d'après le lemme 44, on aura aussi $\left\{\frac{\mathfrak{q}}{\mathfrak{p}}\right\} \neq 1$, $\varkappa$ désignant un nombre primaire de $\mathfrak{q}$ et $\varkappa^e$ une puissance de $\varkappa$ telle que l'on ait $\left\{\frac{\mu\varkappa^e}{\mathfrak{p}}\right\} = 1$, on a, d'après ce qui précède,

$$\prod_{(\mathfrak{w})}' \left\{ \frac{\pi, \mu\varkappa^e}{\mathfrak{w}} \right\} = 1,$$

et comme on a aussi, d'après le lemme 47,

$$\prod_{(\mathfrak{w})}' \left\{ \frac{\pi, \varkappa}{\mathfrak{w}} \right\} = \left\{ \frac{\mathfrak{q}}{\mathfrak{p}} \right\}^{-1} \left\{ \frac{\mathfrak{p}}{\mathfrak{q}} \right\} = 1,$$

on a encore

(180) $$\prod_{(\mathfrak{w})}' \left\{ \frac{\pi, \mu}{\mathfrak{w}} \right\} = 1;$$

le lemme 48 est donc aussi démontré lorsque ν est un nombre primaire d'un idéal de première espèce. Des égalités (175), (179), (180) résulte sa complète généralité.

§ 170. — Le symbole $\{\nu, \mu\}$ et la loi de réciprocité entre deux idéaux premiers quelconques.

Nous arrivons maintenant d'une manière très simple à la nouvelle base de la théorie des corps kummeriens réguliers annoncée au début de ce chapitre. Posons, ν et μ étant deux entiers de $c(\zeta)$,

(181) $$\{\nu, \mu\} = \prod_{(\mathfrak{w})}' \left\{ \frac{\nu, \mu}{\mathfrak{w}} \right\}^{-1},$$

le produit $\prod_{(\mathfrak{w})}'$ étant encore étendu à tous les idéaux premiers de $c(\zeta)$ différents de $\mathfrak{l}$;

le *symbole* $\left\{\nu, \mu\right\}$ représente ainsi une racine $l^{\text{ième}}$ de l'unité complètement déterminée par les nombres ν, μ, et on tire de (80) les formules

$$(182)\quad \left\{\begin{aligned} &\left\{\nu_1\nu_2, \mu\right\} = \left\{\nu_1, \mu\right\}\left\{\nu_2, \mu\right\},\\ &\left\{\nu, \mu_1\mu_2\right\} = \left\{\nu, \mu_1\right\}\left\{\nu, \mu_2\right\},\\ &\left\{\nu, \mu\right\}\left\{\mu, \nu\right\} = 1,\end{aligned}\right.$$

ν, ν_1, ν_2, μ, μ_1, μ_2 étant des entiers quelconques de $c(\zeta)$. r désignant ensuite une racine primitive mod l et $s = (\zeta : \zeta^r)$ la substitution correspondante du groupe de $c(\zeta)$, on a

$$(183)\quad \left\{s\nu, s\mu\right\} = \left\{\nu, \mu\right\}^r.$$

On a ensuite la proposition

Lemme 49. — Si ν, μ sont deux nombres primaires de $c(\zeta)$, le symbole $\left\{\nu, \mu\right\}$ a toujours la valeur 1.

Démonstration. — On a d'abord, a étant un entier rationnel quelconque premier à l et à ν (théorème 140), l'égalité

$$(184)\quad \left\{\nu, a\right\} = \left\{\frac{\nu}{a}\right\}^{-1}\left\{\frac{a}{\nu}\right\} = 1.$$

μ devant être primaire, $\mu . s^{\frac{l-1}{2}}\mu$ est congru mod $\mathfrak{l}^{l-1}$ à un entier rationnel. On peut, par suite, déterminer un entier rationnel a tel que l'on ait la congruence

$$a . \mu . s^{\frac{l-1}{2}}\mu \equiv 1, \quad (\mathfrak{l}^l),$$

et que de plus a soit premier à ν. On obtient alors, en appliquant le lemme 48,

$$\left\{\nu, a\right\}\left\{\nu, \mu\right\}\left\{\nu, s^{\frac{l-1}{2}}\mu\right\} = \left\{\nu, a . \mu . s^{\frac{l-1}{2}}\mu\right\} = 1,$$

et par suite aussi, vu (184),

$$\left\{\nu, \mu\right\}\left\{\nu, s^{\frac{l-1}{2}}\mu\right\} = 1.$$

On démontre de même

$$\left\{\nu, s^{\frac{l-1}{2}}\mu\right\}\left\{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu\right\} = 1.$$

Puis on tire de (183)

$$\left\{\nu, \mu\right\}\left\{s^{\frac{l-1}{2}}\nu, s^{\frac{l-1}{2}}\mu\right\} = 1.$$

Les trois dernières égalités réunies donnent

$$\left\{\nu, \mu\right\}^2 = 1, \quad \text{c'est-à-dire} \quad \left\{\nu, \mu\right\} = 1. \qquad \text{C. q. f. d.}$$

Si l'on choisit, en particulier pour ν, μ, des nombres primaires de deux idéaux premiers quelconques $\mathfrak{p}$, $\mathfrak{q}$ de $c(\zeta)$, l'énoncé du lemme 49 est équivalent à la loi générale de réciprocité 161 pour ces idéaux premiers.

§ 171. — Coïncidence des symboles $\{\nu, \mu\}$ et $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$.

Nous déduisons du théorème 151, dont le cas $\mathfrak{w} = \mathfrak{l}$ est seul utilisé, que $\{\nu, \mu\}$ a toujours la valeur 1 si ν est norme relative d'un entier du corps $c(\sqrt[l]{\mu}, \zeta)$; et nous arrivons enfin maintenant à montrer que $\{\alpha, \mu\}$ a aussi la valeur 1 si α est reste de normes du corps $c(\sqrt[l]{\mu}, \zeta)$. En effet, supposons pour abréger que les deux nombres α, μ soient premiers à $\mathfrak{l}$ et posons $\alpha = N_c(A)$, mod $\mathfrak{l}^l$, A étant un entier de $c(\sqrt[l]{\mu}, \zeta)$, le nombre $\alpha . (N_c(A))^{l-1}$ est évidemment congru à la $l^{\text{ième}}$ puissance d'un entier mod $\mathfrak{l}^l$; par suite on a, en utilisant les formules (182), les remarques faites et le lemme 48,

$$\{\alpha(N_c(A))^{l-1}, \mu\} = \{\alpha, \mu\}\{N_c(A), \mu\}^{l-1} = \{\alpha, \mu\} = 1,$$

comme nous l'avions annoncé. Si l'un des nombres α, μ ou tous les deux sont divisibles par $\mathfrak{l}$, la démonstration se fait aussi sans difficulté au moyen des mêmes procédés.

Si μ est un entier de $c(\zeta)$ premier à $\mathfrak{l}$, on tire aisément de (181)

$$\{\zeta, \mu\} = \zeta^{\frac{1-n(\mu)}{l}};$$

par suite, l'expression $\{\nu, \mu\}$ remplit toutes les conditions que remplit le symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ (fin du § 133); on a donc, en prenant la définition du symbole $\left(\frac{\nu, \mu}{\mathfrak{l}}\right)$ donnée paragraphe 133,

$$\{\nu, \mu\} = \left(\frac{\nu, \mu}{\mathfrak{l}}\right);$$

on retrouve dans cette égalité le théorème 163.

Si les deux nombres ν, μ sont premiers à $\mathfrak{l}$ et que $\bar{\nu}$, $\bar{\mu}$ désignent des entiers de $c(\zeta)$ vérifiant les congruences

$$\nu \equiv \bar{\nu}, \quad \mu \equiv \bar{\mu}, \quad (\text{mod } \mathfrak{l}^l),$$

on obtient facilement, à l'aide du lemme 48,

$$\left(\frac{\nu, \mu}{\mathfrak{l}}\right) = \left(\frac{\bar{\nu}, \bar{\mu}}{\mathfrak{l}}\right).$$

De là et de la considération des formules (182) nous tirons le résultat suivant :

Si les deux nombres ν, μ sont premiers à $\mathfrak{l}$ et si l'on pose

$$\nu \equiv a^l(1+\lambda)^{n_1}(1+\lambda^2)^{n_2}\dots(1+\lambda^{l-1})^{n_{l-1}}, \quad (\text{mod } \mathfrak{l}^l),$$
$$\mu \equiv b^l(1+\lambda)^{m_1}(1+\lambda^2)^{m_2}\dots(1+\lambda^{l-1})^{m_{l-1}}, \quad (\text{mod } \mathfrak{l}^l),$$

a, b et les exposants n et m étant des entiers rationnels, on a une égalité de la forme

$$\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = \zeta^{L(n_1,\ \ldots,\ n_{l-1};\ m_1,\ \ldots,\ m_{l-1})},$$

L étant ici une fonction bilinéaire homogène des deux séries de variables n_1, ..., n_{l-1}, m_1, ..., m_{l-1}, et les coefficients de L sont des entiers rationnels ne dépendant que du nombre premier l et faciles à calculer pour une valeur donnée de l en prenant des valeurs particulières pour ν et μ.

Après avoir défini le symbole $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ et établi ses propriétés les plus importantes, nous pouvons laisser de côté la restriction maintenue jusqu'à présent dans ce chapitre pour les corps kummeriens d'avoir leur discriminant relatif premier à $\mathfrak{l}$; c'est ce qu'on parvient à démontrer, comme plus haut, en s'appuyant sur les théorèmes 164, 165, 166 et surtout sur le théorème fondamental 167. Ce dernier et le théorème 152 permettent de montrer ensuite que ν, μ étant deux entiers quelconques de $c(\zeta)$, tels que l'on ait $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\} = 1$, et que μ ne soit pas égal à la $l^{\text{ème}}$ puissance d'un nombre de $c(\zeta)$, le nombre ν est toujours résidu de normes, mod $\mathfrak{l}$, du corps kummerien $c(\sqrt[l]{\mu},\ \zeta)$. Par suite le théorème 151 est vérifié par surcroît pour $\mathfrak{w} = \mathfrak{l}$, ainsi par conséquent que le théorème 150 pour $\mathfrak{w} = \mathfrak{l}$. Avec cette nouvelle manière d'édifier la théorie des corps kummeriens réguliers, ces théorèmes 150 et 151 pour $\mathfrak{w} = \mathfrak{l}$ paraissent les clés de voûte de toute la construction, contrairement à la première méthode.

CHAPITRE XXXVI.

L'équation diophantine $\alpha^m + \beta^m + \gamma^m = 0$.

§ 172. Impossibilité de l'équation $\alpha^l + \beta^l + \gamma^l = 0$ pour les exposants premiers réguliers l.

Fermat a émis l'assertion que l'équation

$$a^m + b^m + c^m = 0$$

est impossible en nombres entiers a, b, c différents de 0 pour tout exposant entier $m > 1$. Bien que déjà avant Kummer on ait obtenu des résultats isolés remarquables sur cette équation de Fermat [Abel[1], Cauchy[1,2], Dirichlet[1,2,3], Lamé[1,2,3], Lebesque[1,2,3]], c'est pourtant Kummer qui est parvenu le premier, en s'appuyant sur la théorie des idéaux des corps circulaires réguliers, à démontrer le théorème de Fermat pour des classes très étendues d'exposants m. Le plus important des résultats de Kummer est le suivant :

Théorème 168. — l étant un nombre premier régulier et α, β, γ des entiers quelconques du corps circulaire des racines $l^{\text{ièmes}}$ de l'unité, dont aucun n'est nul, on n'a jamais l'égalité

(185) $$\alpha^l + \beta^l + \gamma^l = 0.$$

[Kummer[1, 9, 11].]

Démonstration. — Soit $\zeta = e^{\frac{2i\pi}{l}}$, $\lambda = 1 - \zeta$, $\mathfrak{l} = (\lambda)$. Supposons que l'équation (185) ait une solution en nombres entiers α, β, γ du corps $c(\zeta)$ et distinguons les deux cas où aucun des trois entiers α, β, γ n'est divisible par $\mathfrak{l}$ et celui où l'un au moins des trois est divisible par $\mathfrak{l}$.

Dans le *premier* cas, on doit en tout cas exclure les valeurs 3 et 5 pour l'exposant l. En effet, pour $l = 3$ chacun des trois nombres α, β, γ serait $\equiv \pm 1$, mod $\mathfrak{l}$, et par suite chacune des trois puissances α^3, β^3, $\gamma^3 \equiv \pm 1$, mod $\mathfrak{l}^3$; la somme $\alpha^3 + \beta^3 + \gamma^3$ serait donc congrue à ± 1 ou à ± 3, mod $\mathfrak{l}^3$, ce qui est incompatible avec l'équation (185). On arrive à une contradiction semblable avec $l = 5$, si l'on considère que dans ce cas chacun des trois nombres α, β, γ est congru, mod $\mathfrak{l}$, à ± 1 ou ± 2, et par suite chacune des trois puissances α^5, β^5, γ^5 devrait être congrue à ± 1, ± 32, mod $\mathfrak{l}^5$ (¹).

Soit donc $l \geqslant 7$. Si l'équation (185) est vérifiée par les trois nombres α, β, γ, on a évidemment aussi $\alpha^{*l} + \beta^{*l} + \gamma^{*l} = 0$, en désignant par α^*, β^*, γ^* les produits de α, β, γ par des racines $l^{\text{ièmes}}$ quelconques de l'unité. Cela étant, nous pouvons dorénavant admettre que les trois nombres α, β, γ vérifiant l'équation (185) sont semi-primaires. Mettons alors l'équation (185) sous la forme

(186) $$(\alpha + \beta)(\alpha + \zeta\beta)(\alpha + \zeta^2\beta) \ldots (\alpha + \zeta^{l-1}\beta) = -\gamma^l.$$

Si deux facteurs du premier membre, par exemple $\alpha + \zeta^u\beta$ et $\alpha + \zeta^{u+g}\beta$, avaient un facteur commun, celui-ci devrait aussi diviser $(\zeta^g - 1)\alpha$ et $(1 - \zeta^g)\beta$, et comme $\frac{1 - \zeta^g}{1 - \zeta}$ est une unité et que $\mathfrak{l}$ ne divise pas γ, ce facteur commun devrait nécessaire-

(¹) N. T. — Pour $l = 7$, la contradiction relevée dans le premier cas pour $l = 3$, $l = 5$ n'existe pas. En prenant, en effet,

$$\alpha \equiv -1, \quad \beta \equiv -2, \quad \gamma \equiv +3, \qquad \text{mod } \mathfrak{l},$$

on a

$$\alpha^7 \equiv -1, \quad \beta^7 \equiv -128, \quad \gamma^7 \equiv +2187, \quad \text{mod } (\mathfrak{l}^7 = 7.\mathfrak{l}),$$

et

$$0 \equiv \alpha^7 + \beta^7 + \gamma^7 \equiv 2058 \quad \text{ou} \quad 7 \times 294 = 7 \times 7 \times 42, \quad \text{mod } 7.\mathfrak{l},$$

ou

$$7 \times 42 \equiv 0, \quad \text{mod } \mathfrak{l},$$

congruence qui est vérifiée.

ment appartenir aux nombres α et β. Tout facteur premier ne figurant que dans un seul des l facteurs du premier membre de (186) doit évidemment, d'après cette équation même, avoir un exposant multiple de l; les l facteurs du premier membre de (186) se décomposent donc comme suit :

$$\begin{aligned}
\alpha + \beta \quad &= \mathfrak{j}^l \mathfrak{a}, \\
\alpha + \zeta\beta \quad &= \mathfrak{j}_1^l \mathfrak{a}, \\
\alpha + \zeta^2\beta \quad &= \mathfrak{j}_2^l \mathfrak{a}, \\
\cdots &\cdots \\
\alpha + \zeta^{l-1}\beta &= \mathfrak{j}_l^{l-1}\mathfrak{a},
\end{aligned}$$

$\mathfrak{a}$ désignant le plus grand commun diviseur idéal des nombres α et β, et $\mathfrak{j}$, $\mathfrak{j}_1$, ..., $\mathfrak{j}_{l-1}$ des idéaux de $c(\zeta)$. Comme $\alpha + \zeta^{l-1}\beta$, en particulier, est premier à $\mathfrak{l}$, on peut déterminer une racine $l^{\text{ième}}$ de l'unité ζ^*, telle que $\zeta^*(\alpha + \zeta^{l-1}\beta)$ soit semi-primaire. Posons

$$\mu = \frac{\alpha}{\zeta^*(\alpha + \zeta^{l-1}\beta)}, \qquad \rho = \frac{\beta}{\zeta^*(\alpha + \zeta^{l-1}\beta)}.$$

On obtient alors

$$(187) \qquad \left\{\begin{aligned}
\mu + \rho \quad &= \left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l, \\
\mu + \zeta\rho \quad &= \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l, \\
\cdots &\cdots \\
\mu + \zeta^{l-2}\rho &= \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l,
\end{aligned}\right.$$

c'est-à-dire que l'on a

$$\left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l \sim 1, \quad \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l \sim 1, \quad \ldots, \quad \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^l \sim 1,$$

et on a de plus

$$(188) \qquad \mu + \zeta^{l-1}\rho = \zeta^{*-1}.$$

h désignant le nombre des classes d'idéaux de $c(\zeta)$, on a, d'autre part,

$$\left(\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^h \sim 1, \quad \left(\frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^h \sim 1, \quad \ldots, \quad \left(\frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}}\right)^h \sim 1;$$

et, *comme h est premier à l*, on en déduit

$$\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}} \sim 1, \quad \ldots, \quad \frac{\mathfrak{j}_{l-2}}{\mathfrak{j}_{l-1}} \sim 1.$$

Par conséquent, on peut (voir théorème 127, § 98) mettre les relations (187) sous la forme

$$(189) \qquad \mu + \zeta^u\rho = \zeta^{e_u}\varepsilon_u\alpha_u^l, \qquad (u = 0, 1, 2, \ldots, l-2),$$

les e_u désignant des exposants entiers rationnels, les ε_u des unités *réelles* du corps circulaire $c(\zeta)$ et les α_u des nombres de $c(\zeta)$ entiers ou fractionnaires à numérateurs et dénominateurs premiers à $\mathfrak{l}$. La $l^{ième}$ puissance du nombre α_u étant toujours congrue à un certain entier rationnel a_u, mod $\mathfrak{l}^l$ [1], on tire des égalités (189) les congruences

(190) $$\mu + \zeta^u \rho \equiv \zeta^{e_u} \varepsilon_u \alpha_u, \quad (\mathfrak{l}^l), \qquad (u = 1, 2, \ldots, l-2).$$

Effectuons dans ces congruences la substitution $(\zeta : \zeta^{-1})$ et désignons par μ' et ρ' les transformés de μ et ρ par cette substitution ; il vient

(191) $$\mu' + \zeta^{-u} \rho' \equiv \zeta^{-e_u} \varepsilon_u a_u, \quad (\mathfrak{l}^l), \qquad (u = 1, 2, \ldots, l-2).$$

De (190) et (191) résulte

(192) $$\mu + \zeta^u \rho \equiv \zeta^{2e_u} \mu' + \zeta^{2e_u - u} \rho', \quad (\mathfrak{l}^l), \qquad (u = 1, 2, \ldots, l-2).$$

En posant $\mu \equiv m$, $\rho \equiv r$, mod $\mathfrak{l}^2$, m et r étant des entiers rationnels [2], il résulte

---

[1] N. T. — La puissance $l^{ième}$ de tout nombre α de $c(\zeta)$ est congrue mod $\mathfrak{l}^l$ à un certain entier rationnel a.

En effet, α peut être mis sous la forme

$$\alpha = \frac{a_0 + a_1 \lambda + a_2 \lambda^2 + \ldots + a_{l-2} \lambda^{l-2}}{b_0} \qquad (\text{les } a_i \text{ et } b_0 \text{ étant entiers rationnels}),$$

a_0 et b_0 étant premiers à l ; on a donc :

$$b_0 \alpha \equiv a_0, \quad (\text{mod } \mathfrak{l}).$$

On peut toujours déterminer un entier b tel que l'on ait

$$b b_0 \equiv 1, \quad (\text{mod } l),$$

alors on a

$$b b_0 \alpha \equiv a_0 b, \quad (\text{mod } \mathfrak{l}),$$

c'est-à-dire

$$\alpha \equiv a_0 b, \quad (\text{mod } \mathfrak{l}),$$

et par suite

$$\alpha^l \equiv a, \quad (\text{mod } \mathfrak{l}^l),$$

a étant entier rationnel.

[2] N. T. — En effet,

$$\mu = \frac{a_0 + a_2 \lambda^2 + \ldots + a_{l-2} \lambda^{l-2}}{b_0 + b_2 \lambda^2 + \ldots + b_{l-2} \lambda^{l-2}},$$

car μ est le quotient de deux nombres *semi-primaires*.

$$\mu \equiv m, \quad (\text{mod } \mathfrak{l}^2),$$

revient donc à

$$b_0 m \equiv a_0, \quad (\text{mod } \mathfrak{l}^2) ;$$

or b_0 et a_0 étant premiers à l, la congruence

$$b_0 m \equiv a_0, \quad (\text{mod } l),$$

a toujours une solution $m \not\equiv 0$, et par suite l'on a aussi

$$b_0 m \equiv a_0, \quad (\text{mod } \mathfrak{l}^2).$$

de (192)

(193) $$m + \zeta^{u} r \equiv \zeta^{2e_u} m + \zeta^{2e_u - u} r, \quad (\mathfrak{l}^2).$$

et, à cause de la relation générale $\zeta^{g} \equiv 1 - g\lambda$, mod $\mathfrak{l}^2$, (193) donne la congruence

$$2e_u(m + r) \equiv 2ru, \quad (\text{mod } l).$$

D'autre part, il résulte de l'égalité (188) : $m + r \equiv 1$, mod l, et par suite nous avons

$$e_u \equiv ru, \quad (\text{mod } l), \qquad (u = 0, 1, 2, \ldots, l-2)$$

Prenons alors, en tenant compte de cette relation, les congruences (192) pour $u = 0, 1, 2, 3$; on en tire, en éliminant μ, ρ, μ', ρ',

$$\begin{vmatrix} 1, & 1, & 1, & 1 \\ 1, & \zeta, & \zeta^{2r}, & \zeta^{2r-1} \\ 1, & (\zeta)^2, & (\zeta^{2r})^2, & (\zeta^{2r-1})^2 \\ 1, & (\zeta)^3, & (\zeta^{2r})^3, & (\zeta^{2r-1})^3 \end{vmatrix} \equiv 0, \quad (\text{mod } \mathfrak{l}^l),$$

c'est-à-dire

(194) $$(1 - \zeta)(1 - \zeta^{2r})(1 - \zeta^{2r-1})(\zeta - \zeta^{2r})(\zeta - \zeta^{2r-1})(\zeta^{2r} - \zeta^{2r-1}) \equiv 0, \quad (\mathfrak{l}^l).$$

Aucun des facteurs du premier membre n'est égal à o, car autrement on aurait soit $r \equiv 0$, soit $r \equiv 1$, soit $r \equiv \frac{1}{2}$, mod l. Si l'on avait $r \equiv 0$, mod l, il en résulterait $\beta \equiv 0$, mod $\mathfrak{l}$; si l'on avait $r \equiv 1$, mod l, il en résulterait $\rho \equiv 1$, mod $\mathfrak{l}$, c'est-à-dire $\beta \equiv \alpha + \beta$ ou $\alpha \equiv 0$, mod $\mathfrak{l}$. Dans les deux cas c'est impossible, vu notre hypothèse sur les nombres α, β, γ. Si l'on avait $r \equiv \frac{1}{2}$, mod $\mathfrak{l}$, on aurait $\rho \equiv \frac{1}{2}$, mod $\mathfrak{l}$, c'est-à-dire $2\beta \equiv \alpha + \beta$ ou $\alpha \equiv \beta$, mod $\mathfrak{l}$. Mais comme α, β, γ entrent symétriquement dans l'équation (185), on aurait aussi $\alpha \equiv \beta \equiv \gamma$, mod $\mathfrak{l}$, et par suite

$$\alpha^l + \beta^l + \gamma^l \equiv 3\alpha \equiv 0,$$

c'est-à-dire $\alpha \equiv 0$, mod $\mathfrak{l}$, contrairement encore à l'hypothèse. Chaque facteur du premier membre de la congruence (194) est par suite divisible par $\mathfrak{l}$, mais non par $\mathfrak{l}^2$; cette congruence est donc impossible, puisqu'on a $l \geqslant 7$.

Supposons maintenant, *en second lieu*, que dans l'équation (185) l'un des trois nombres α, β, γ, par exemple γ, soit divisible par $\mathfrak{l}$ et contienne ce facteur à la $m^{\text{ième}}$ puissance. Si l'on remplace alors γ par $\lambda^m \delta$, δ étant un entier de $c(\zeta)$ premier à $\mathfrak{l}$, l'équation (185) prend la forme

(195) $$\alpha^l + \beta^l = \varepsilon \lambda^{lm} \delta^l,$$

ε étant ici égal à -1. On va montrer qu'une équation de cette forme (195) est même impossible, α, β, δ étant des entiers quelconques de $c(\zeta)$ premiers à $\mathfrak{l}$ et ε une unité *quelconque* du corps circulaire $c(\zeta)$. Pour cela, supposons encore les nombres α, β

semi-primaires et observons d'abord que α^l, β^l sont congrus à des entiers rationnels, mod $\mathfrak{l}^{l-1}$, et que, vu (195), $\varepsilon\lambda^{ml}\delta^l$ doit aussi être congru à un entier rationnel, mod $\mathfrak{l}^{l-1}$; m doit donc être > 1. On trouve ensuite, par des considérations analogues à celles du cas précédent et en tenant compte de ce que $\alpha + \beta$ est semi-primaire, les égalités

$$(196)\quad \begin{cases} \alpha + \beta = \lambda^{l(m-1)+1}\mathfrak{j}^l\mathfrak{a}, \\ \alpha + \zeta\beta = \lambda\mathfrak{j}_1^l\mathfrak{a}, \\ \dots\dots\dots\dots \\ \alpha + \zeta^{l-1}\beta = \lambda\mathfrak{j}_{l-1}^l\mathfrak{a}, \end{cases}$$

où $\mathfrak{j}$, $\mathfrak{j}_1$, …, $\mathfrak{j}_{l-1}$, $\mathfrak{a}$ sont des idéaux premiers à $\mathfrak{l}$ de $k(\zeta)$. Si $l = 3$, le nombre de classes h du corps $k(\zeta)$ est égal à 1 et, par suite, tout idéal de $k(\zeta)$ est un idéal principal. En posant dans ce cas $\mathfrak{a} = (\varkappa)$, $\varkappa$ étant un entier de $k(\zeta)$, et ensuite

$$\mu = \frac{\alpha}{\varkappa}, \quad \rho = \frac{\beta}{\varkappa},$$

les égalités (196) deviennent

$$(197)\quad \begin{cases} \mu + \rho = \lambda^{l(m-1)+1}\mathfrak{j}^l, \\ \mu + \zeta\rho = \lambda\mathfrak{j}_1^l, \\ \mu + \zeta^2\rho = \lambda\mathfrak{j}_2^l. \end{cases}$$

Dans le cas de $l > 3$, formons les nombres

$$\mu = \frac{\alpha\lambda}{\alpha + \zeta^{l-1}\beta}, \quad \rho = \frac{\beta\lambda}{\alpha + \zeta^{l-1}\beta};$$

on peut aussi les mettre sous forme de fractions dont le numérateur et le dénominateur soient premiers à $\mathfrak{l}$. Les trois premières et la dernière des égalités (196) nous donnent

$$(198)\quad \begin{cases} \mu + \rho = \lambda^{l(m-1)+1}\left(\dfrac{\mathfrak{j}}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu + \zeta\rho = \lambda\left(\dfrac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}}\right)^l, \\ \mu + \zeta^2\rho = \lambda\left(\dfrac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}}\right)^l. \end{cases}$$

Nous en concluons encore

$$\frac{\mathfrak{j}}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_1}{\mathfrak{j}_{l-1}} \sim 1, \quad \frac{\mathfrak{j}_2}{\mathfrak{j}_{l-1}} \sim 1,$$

et par suite nous pouvons mettre les égalités (198) sous la forme

$$(199)\quad \begin{cases} \mu + \rho = \dfrac{\varepsilon^* \lambda^{l(m-1)-1} \gamma^{*l}}{\nu}, \\[2ex] \mu + \zeta\rho = \dfrac{\lambda \alpha^{*l}}{\nu}, \\[2ex] \mu + \zeta^2\rho = \dfrac{\varepsilon\lambda\beta^{*l}}{\nu}, \end{cases}$$

ν, α^*, β^*, γ^* étant des entiers de $c(\zeta)$ premiers à $\mathfrak{l}$ et ε et ε^* des unités de ce corps. A cause de (197), on a également, si $l=3$, un système comme (199). En éliminant μ et ρ, on obtient, aussi bien pour $l=3$ que pour $l>3$, une équation de la forme

$$(200)\quad \alpha^{*l} + \eta\beta^{*l} = \eta^*\lambda^{l(m-1)}\gamma^{*l},$$

où η et η^* (égales à $-\dfrac{1-\zeta}{1-\zeta^2}\varepsilon$ et à $-\dfrac{\zeta(1-\zeta)}{1-\zeta^2}\varepsilon^*$) sont des unités de $c(\zeta)$. α^{*l}, β^{*l} étant congrus mod $\mathfrak{l}^l$ à des entiers rationnels et m étant >1, comme on l'a démontré, il résulte de cette équation (200) que η aussi doit être congru à un entier rationnel mod $\mathfrak{l}^l$, et par suite (théorème 156, § 141) η est la $l^{\text{ième}}$ puissance d'une unité de $c(\zeta)$. En mettant alors $\beta^*\eta^{\frac{1}{l}}$ à la place de β^* dans (200) cette équation prend la forme de (195), sauf que l'exposant m a diminué d'une unité. En continuant ce procédé, on finirait par arriver à une équation de la forme (195) avec $m=1$, et par suite par arriver à une contradiction. Le théorème 168 est donc complètement démontré.

§ 173. Autres recherches sur l'impossibilité de $\alpha^m + \beta^m + \gamma^m = 0$.

Kummer a encore donné la démonstration de l'impossibilité de l'équation

$$\alpha^l + \beta^l + \gamma^l = 0$$

en nombres entiers α, β, γ du corps circulaire des racines $l^{\text{ièmes}}$ de l'unité, dans le cas où l est un nombre premier divisant le nombre de classes h du corps circulaire $c\left(e^{\frac{2i\pi}{l}}\right)$, h n'étant d'ailleurs pas divisible par l^2 (¹). [Kummer[16].] D'après la remarque paragraphe 139, le théorème de Fermat est donc reconnu exact pour tous les exposants $m \leqslant 100$. La démonstration de la proposition de Fermat dans toute sa généralité est encore à trouver.

Il reste encore à traiter le cas où l'exposant m est une puissance de 2. L'équation $a^2+b^2=c^2$ a, comme on sait, une infinité de solutions en nombres entiers rationnels a, b, c. Cependant, on a ensuite le

---

(¹) N. T. — Voir, pour cette démonstration, la note VI.

THÉORÈME 169. — α, β, γ étant des entiers $\neq 0$ du corps quadratique déterminé par $i = \sqrt{-1}$, on n'a jamais l'équation

$$\alpha^4 + \beta^4 = \gamma^2. \tag{201}$$

Démonstration. — Admettons qu'il existe, au contraire, trois entiers α, β, γ vérifiant cette équation. Posons $\lambda = 1 + i$ et $\mathfrak{l} = (\lambda)$. Nous voyons d'abord facilement que l'un des deux nombres α, β doit être divisible par λ. En effet, admettons que α et β soient premiers à λ et observons qu'un entier de $c(i)$ premier à λ est toujours $\equiv 1$ ou i, mod $\mathfrak{l}^2$; son carré est par suite $\equiv \pm 1$, mod $\mathfrak{l}^4$, et sa quatrième puissance est $\equiv 1$ mod $\mathfrak{l}^6$. Il en résulte $\alpha^4 + \beta^4 \equiv 2$, mod $\mathfrak{l}^6$. Par suite, γ devrait être divisible par $\mathfrak{l}$ et non par $\mathfrak{l}^2$. Mais si nous posons en conséquence $\gamma = \lambda + \lambda^2\gamma'$, γ' étant encore un entier de $c(i)$, nous trouvons $\gamma^2 \equiv 2i$, mod $\mathfrak{l}^4$, et par suite toujours $\gamma^2 \not\equiv \alpha^4 + \beta^4$, mod $\mathfrak{l}^4$, contrairement à l'hypothèse. Le cas où les deux nombres α et β seraient divisibles par $\mathfrak{l}$ peut évidemment être exclu de suite, car alors γ serait divisible par $\mathfrak{l}^2$ et on pourrait supprimer la puissance λ^4 dans les deux membres de l'équation (201).

Il ne reste donc que le cas où un des nombres α, β, par exemple α, est divisible par $\mathfrak{l}$, β et γ étant au contraire premiers à $\mathfrak{l}$. Nous posons $\alpha = \lambda^m\alpha^*$, où α^* est un nombre premier à λ, et nous considérons l'équation plus générale

$$\beta^4 - \gamma^2 = \varepsilon\lambda^{4m}\alpha^{*4}, \tag{202}$$

ε désignant une unité de $c(i)$. Nous déduisons de cette équation (202), en changeant au besoin γ en $-\gamma$, deux équations de la forme

$$\left\{\begin{aligned} \beta^2 + \gamma &= \eta\lambda^{4m-2}\alpha'^4, \\ \beta^2 - \gamma &= \vartheta\lambda^2\beta'^4, \end{aligned}\right. \tag{203}$$

où η, ϑ sont des unités de $c(\zeta)$, α' et β' des entiers de $c(i)$ premiers à $\mathfrak{l}$. En additionnant les deux équations (203) et divisant le résultat par $\vartheta\lambda^2$, on obtient une équation

$$\beta'^4 - \vartheta'\beta^2 = \eta'\lambda^{4m-4}\alpha'^4 \tag{204}$$

où ϑ', η' sont des unités de $c(i)$. Si m était égal à 1, cette équation serait sûrement impossible, car $\beta', \vartheta', \beta, \eta', \alpha'$ sont tous $\equiv 1$ mod $\mathfrak{l}$. Donc on a $m > 1$. Mais alors on déduit de cette équation (204) la congruence $\vartheta' \equiv 1$ mod $\mathfrak{l}^2$; par suite, on a $\vartheta' = \pm 1$. En posant $\beta = \gamma'$ ou $\beta = i\gamma'$, suivant que $\vartheta = +1$ ou -1, l'équation (204) prend la forme (202), à part que m a diminué de 1. En continuant ainsi, on arrive à une contradiction.

On déduit immédiatement du théorème de Fermat pour $l = 3$ qu'il n'existe au

cune équation du troisième degré à coefficients rationnels et de discriminant 1 en dehors des deux suivantes :

$$x^3 - x \pm \frac{1}{3} = 0$$

et de celles qui s'en déduisent par la substitution $x = x' + a$ (a étant rationnel). [Kronecker[8].]

On peut, comme Hurwitz, exprimer le théorème de Fermat en disant que l'expression $\sqrt[m]{1 - x^m}$ représente toujours un nombre incommensurable pour m entier > 2 et x fractionnaire positif.

THÉORIE

DES

CORPS DE NOMBRES ALGÉBRIQUES

MÉMOIRE de M. David Hilbert,

Professeur à l'Université de Gœttingen.

NOTES DE MM. G. HUMBERT ET Th. GOT.

NOTE I (annexe au § 5),

Par G. HUMBERT [1].

Démonstration du lemme 2. (Théorème d'Hurwitz.)

Soient

$$F = \alpha_0 x^m + \alpha_1 x^{m-1} + \ldots + \alpha_m,$$
$$G = \beta_0 x^n + \beta_1 x^{n-1} + \ldots + \beta_n,$$

deux polynômes en x, à coefficients entiers algébriques quelconques; soit

$$FG = \gamma_0 x^{m+n} + \gamma_1 x^{m+n-1} + \ldots + \gamma_{m+n};$$

je dis que si un même entier algébrique ω divise tous les γ_i (c'est-à-dire si les $\gamma_i : \omega$, qui sont algébriques, sont aussi entiers), ω divise tous les produits $\alpha_i \beta_k$.

En effet, *fixons i et k*; on a, en désignant par x_h les racines de $F = 0$, par y_h celles de $G = 0$,

$$\pm \frac{\alpha_i}{\alpha_0} \cdot \frac{\beta_k}{\beta_0} = (\Sigma x_1 x_2 \ldots x_i)(\Sigma y_1 y_2 \ldots y_k).$$

---

[1] Cette Note et les suivantes n'ont rien de personnel; elles ont été rédigées, après lecture des Ouvrages ou Mémoires classiques, à l'occasion d'un cours professé au Collège de France en 1910-1911.

Or, considérons l'équation $FG = 0$; soient $\xi_1, \xi_2, \ldots$ ses racines, qui sont les x_h et les y_h; partageons les ξ en deux groupes de toutes les manières possibles, l'un de m racines, l'autre de n; soient ζ_h et η_h les racines de deux groupes d'un même système. La fonction $u = (\Sigma \zeta_1 \zeta_2 \ldots \zeta_i)(\Sigma \eta_1 \eta_2 \ldots \eta_k)$ est une fonction rationnelle *non symétrique* des racines ξ; en prenant tous les groupements possibles des $m+n$ racines ξ en deux groupes de m et n respectivement, on obtient un certain nombre de fonctions u, dont l'une est $\pm \frac{\alpha_i}{\alpha_0} \cdot \frac{\beta_k}{\beta_0}$. D'ailleurs, toute fonction symétrique des u l'est des ξ; donc, les u sont racines d'une équation algébrique dont les coefficients sont rationnels par rapport aux coefficients γ de $FG = 0$. D'une manière plus précise, les coefficients en question sont des polynômes en $\gamma_i : \gamma_0$ à coefficients entiers ordinaires : cela résulte de la proposition suivante facile à démontrer :

Soit une équation algébrique $x^n + a_1 x^{n-1} + \ldots + a_n = 0$; considérons la fonction symétrique des racines x_i : $\Sigma x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, les α_i entiers ordinaires non négatifs : elle s'exprime par un polynôme en $a_1, a_2, \ldots, a_n$, *dont le degré est le plus grand des* α_i et dont les coefficients sont entiers ordinaires.

Soit donc

$$u^M + d_1 u^{M-1} + \ldots + d_M = 0$$

l'équation en u; on a

$$-d_1 = \Sigma u = \Sigma[(\Sigma \zeta_1 \zeta_2 \ldots \zeta_i)(\Sigma \eta_1 \eta_2 \ldots \eta_k)].$$

Le second membre est une fonction symétrique des ξ_i, où les ξ_i figurent tous *au premier degré chacun*; donc, d'après la proposition qui vient d'être énoncée, d_1 est un polynôme d'ordre un par rapport à *l'ensemble* des $\gamma_i : \gamma_0$. De même d_2 est d'ordre deux, d_3 est d'ordre trois, etc.

On peut donc écrire l'équation en u :

$$u^M + \frac{P_1}{\gamma_0} u^{M-1} + \frac{P_2}{\gamma_0^2} u^{M-2} + \ldots + \frac{P_M}{\gamma_0^M} = 0,$$

P_i étant un polynôme entier à coefficients entiers ordinaires d'ordre i par rapport à $\gamma_0, \gamma_1, \gamma_2, \ldots$, et *homogène*, puisque d_i était un polynôme d'ordre i en $\gamma_1 : \gamma_0$, $\gamma_2 : \gamma_0$, etc. D'ailleurs, $\alpha_i \beta_k : \alpha_0 \beta_0$ est l'un des u; donc, en posant $\alpha_i \beta_k = v$ et observant que $\alpha_0 \beta_0 = \gamma_0$, on a pour v l'équation

$$\left(\frac{v}{\gamma_0}\right)^M + \frac{P_1}{\gamma_0}\left(\frac{v}{\gamma_0}\right)^{M-1} + \ldots + \frac{P_M}{\gamma_0^M} = 0,$$

c'est-à-dire

$$v^M + P_1 v^{M-1} + P_2 v^{M-2} + \ldots + P_M = 0.$$

Supposons maintenant que les γ_i soient tous divisibles par ω : je dis que v l'est aussi, ou que $\frac{v}{\omega}$ est un entier algébrique. On écrit en effet

$$\left(\frac{v}{\omega}\right)^{M} + \frac{P_1}{\omega}\left(\frac{v}{\omega}\right)^{M-1} + \frac{P_2}{\omega^2}\left(\frac{v}{\omega}\right)^{M-2} + \ldots + \frac{P_M}{\omega^M} = 0.$$

Or, d'après l'hypothèse $\frac{P_1}{\omega}, \frac{P_2}{\omega^2}, \ldots$ sont des entiers algébriques, car P_i étant *homogène*, à coefficients entiers ordinaires, d'ordre i par rapport aux γ et ceux-ci divisibles par ω, $\frac{P_i}{\omega_i}$ est un polynôme entier à coefficients entiers ordinaires par rapport aux entiers algébriques $\frac{\gamma_i}{\omega}$; donc entier algébrique aussi, par un théorème connu. Donc, également d'après un théorème connu, $\frac{v}{\omega}$, racine d'une équation de premier coefficient 1 et à coefficients entiers algébriques, est entier algébrique; ou encore $\alpha_i \beta_k$ est divisible par ω, c'est-à-dire que le quotient $\alpha_i \beta_k : \omega$ est entier algébrique. C. q. f. d.

NOTE II (ANNEXE AU § 5),

PAR G. HUMBERT.

Démonstration du théorème fondamental 8 par la méthode de Hurwitz mentionnée au paragraphe 6.

LEMME 1. — Soit α un nombre fractionnaire du corps de base $(\omega_1, \ldots, \omega_n)$:

$$\alpha = m_1\omega_1 + \ldots + m_n\omega_n,$$

les m_i entiers ou fractionnaires ordinaires. Prenons successivement pour μ les quantités

$$\mu = 0, 1, \ldots, K^n,$$

K entier ordinaire positif plus grand que 1 ; considérons les quantités $\mu\alpha$ et en particulier les parties entières et fractionnaires des μm_i, c'est-à-dire écrivons $\mu m_i = E_i + \rho_i$, E_i entier positif, nul ou négatif et $0 \leq \rho_i < 1$. On appellera E_i la partie entière, ρ_i la partie fractionnaire de μm_i.

Si on divise l'intervalle 0 — 1 en K parties égales, d'amplitude $\frac{1}{K}$ (avec la conven-

tion que o appartient au premier intervalle partiel, $\frac{1}{K}$ au second, et ainsi de suite), chacune des m parties fractionnaires tombe dans l'une de ces K parties égales; or, on peut répartir *a priori* m quantités dont l'ordre est donné, dans K intervalles, de K^m manières différentes (évident en passant de m à $m+1$). D'autre part, en faisant varier μ, ($\mu = 0, 1, \ldots, K^m$), on a $K^m + 1$ systèmes de m parties fractionnaires à répartir successivement dans les K intervalles. Comme $K^m + 1$ est plus grand que K^m, les $K^m + 1$ répartitions ne seront pas toutes distinctes, c'est-à-dire que deux *au moins* d'entre elles seront identiques.

Soient μ' et μ'' les valeurs correspondantes de μ ($\mu'' > \mu'$); les parties fractionnaires de $\mu' m_1$, $\mu'' m_1$ tombent dans un même intervalle de $\frac{1}{K}$; de même celles de $\mu' m_2$, $\mu'' m_2$, etc. On a ainsi

$$\mu'' m_i = e_i'' + \rho_i'', \qquad \mu' m_i = e_i' + \rho_i', \qquad (i = 1, 2, \ldots, m),$$

ρ_i'' et $\rho_i' \geqq 0$ et compris dans le même intervalle de $\frac{1}{K}$; $|\rho_i'' - \rho_i'|$ est donc sûrement $< \frac{1}{K}$.

Si donc on pose $\mu = \mu'' - \mu'$ (μ est *positif et non nul*, puisque $\mu'' > \mu'$), on aura

$$\mu m_i = e_i'' - e_i' + \rho_i'' - \rho_i',$$

c'est-à-dire

$$\mu m_i = E_i + \rho_i,$$

E_i entier positif, nul ou négatif et ρ_i positif, nul ou négatif, mais inférieur à $\frac{1}{K}$ en valeur absolue.

Par suite, étant données m quantités $m_1, m_2, \ldots, m_m$, on peut trouver dans la série $1, 2, \ldots, K^m$ un entier μ (non nul) tel que, pour $i = 1, 2, \ldots, m$, on ait

$$\mu m_i = E_i + \rho_i; \quad E_i \text{ entier et } |\rho_i| < \frac{1}{K}.$$

Lemme 2. — L'entier μ étant ainsi déterminé, on a

$$\begin{aligned} \mu\alpha &= \mu m_1 \omega_1 + \mu m_2 \omega_2 + \ldots \\ &= (E_1 + \rho_1)\omega_1 + (E_2 + \rho_2)\omega_2 + \ldots \end{aligned}$$

E_i entier ordinaire, ρ_i fractionnaire, $|\rho_i| < \frac{1}{K}$, ou

$$\mu\alpha - (E_1\omega_1 + E_2\omega_2 + \ldots) = \rho_1\omega_1 + \rho_2\omega_2 + \ldots.$$

Il résulte de là que

$$|\mu\alpha - E_1\omega_1 - E_2\omega_2 - \ldots| \leqq |\rho_1| \cdot |\omega_1| + |\rho_2| \cdot |\omega_2| + \ldots;$$

donc, si Ω est le maximum du module des ω (c'est-à-dire le plus grand des $|\omega_i|$), on a

$$|\mu\alpha - A| < \frac{m\Omega}{K}.$$

A étant un entier du corps ω. Passant aux conjugués, on a de même, *pour le même* μ :

$$|\mu\alpha' - A'| < \frac{m\Omega'}{K}.$$

. . . .

On a le même μ parce que ce μ ne dépend que de $m_1, m_2, \ldots, m_m$, qui restent les mêmes quand on passe de α à ses conjugués α′, α″, etc.; de même A′ est le conjugué de A, parce que les E_i ne dépendent que des m_i. Maintenant observons que si β est un nombre d'un corps ω, sa norme est ββ′β″ ...; si l'équation en ω a des racines imaginaires, elles sont deux à deux imaginaires conjuguées et il en est de même pour les β correspondants, de sorte qu'on a dans tous les cas

$$|\text{Norme } \beta| = |\beta| \cdot |\beta'| \ldots .$$

Donc, en multipliant membre à membre les inégalités ci-dessus, on a

$$|\text{Norme } (\mu\alpha - A)| < \frac{m^m \Omega\Omega' \ldots}{K^m} < \frac{C^m}{K^m},$$

C étant un entier fixe qui ne dépend que du corps et non du nombre α.

Prenons K = C; il en résulte le lemme suivant :

Etant donné dans un corps d'ordre m un nombre entier ou fractionnaire α, on peut trouver un entier ordinaire μ positif, au plus égal à C^m, (C étant un entier positif ne dépendant que du corps) et un entier A du corps tels que

$$|\text{Norme } (\mu\alpha - A)| < 1.$$

Corollaire. — Soit I un idéal quelconque, α un de ses entiers autre que o *et de norme minimum en valeur absolue* (autre que o nécessairement, car la norme étant αα′ ... ne peut être nulle qui si un des α, donc évidemment tous, sont nuls). Soit α_1 un autre entier de I; appliquons le lemme 2 au nombre du corps $\frac{\alpha_1}{\alpha}$. On aura, pour μ entier ordinaire positif et $\leqslant C^m$,

$$\left|N\left(\mu\frac{\alpha_1}{\alpha} - \beta\right)\right| < 1,$$

β entier du corps, d'où

$$|N(\mu\alpha_1 - \beta\alpha)| < |N\alpha|.$$

Mais $|N\alpha|$ étant en valeur absolue la norme minimum autre que o dans l'idéal et $\mu\alpha_1 - \beta\alpha$ étant un entier de l'idéal, puisque α_1 et α en sont et que μ et β sont entiers du corps, on a nécessairement

$$N(\mu\alpha_1 - \beta\alpha) = 0,$$

d'où

$$\mu\alpha_1 = \beta\alpha$$

par une remarque qu'on vient de faire.

Donc $\gamma\alpha_1$ est divisible par α; *a fortiori*, puisque γ est un des entiers 1, 2, ..., C^m, il en sera de même de $C^m!\,\alpha_1$.

Posant $C^m! = M$, on voit que, α_1 étant un entier quelconque d'un idéal I, $M\alpha_1$ est divisible par α, ou encore que tous les entiers de l'idéal MI sont divisibles par α, ce qui entraîne

$$(M)I = (\alpha)J,$$

J étant un idéal.

Je dis que J contient M. En effet, $(M)I = (\alpha)J$ montre que le produit d'un nombre de I par M, divisé ensuite par α, est un nombre de J; or, α étant de I, l'entier $\frac{\alpha . M}{\alpha} = M$ est de J.

Si donc on dit que deux idéaux I et J sont *équivalents* lorsqu'il existe deux entiers du corps λ et μ tels que $(\lambda)I = (\mu)J$, on peut dire que

Tout idéal équivaut à un idéal qui contient un nombre fixe M *dépendant seulement du corps.*

Remarque. — *Deux idéaux équivalents à un troisième le sont entre eux.* Car si

$$(\alpha)I = (\beta)K,$$

$$(\alpha_1)I_1 = (\beta_1)K,$$

on en conclut

$$(\beta)(\beta_1)K = (\alpha\beta_1)I = (\alpha_1\beta)I_1.$$

Théorème. — *Si on range dans une même classe les idéaux équivalents, le nombre des classes d'idéaux est fini.*

Car tout idéal équivaut à un idéal contenant M, donc contenant (M). Or, un idéal donné, ici (M), n'est contenu que dans un nombre limité d'idéaux (lemme 1 du paragraphe 4); donc le nombre des classes d'idéaux est fini.

Théorème. — *Une puissance convenable d'un idéal quelconque* I *est un idéal principal.*

Formons, en effet, I, I^2, I^3, ... en nombre illimité; il faut, par le théorème précédent, que deux de ces idéaux soient équivalents, c'est-à-dire

$$(\alpha)I^r = (\beta)I^{r+s} = (\beta)I^r . I^s.$$

On n'a pas le droit de diviser par I^r, *parce qu'on ne suppose pas établi le théorème fondamental qu'on peut trouver, pour tout idéal* I, *un autre idéal* J *tel que* IJ *soit principal.* Mais on sait que si un idéal quelconque $J = KL$, tout nombre de J appartient à K, car si ρ_1, ρ_2, ... sont les nombres de K et σ_1, σ_2, ... ceux de L, ceux de KL sont $\Sigma\lambda\rho_i\sigma_j$, et ce sont évidemment des nombres de K; ainsi tout nombre de $KL = J$ est de K.

Soient $\alpha_1, \ldots, \alpha_m$ et $\beta_1, \ldots, \beta_m$ des bases de I^r et $I^{r'}$; il résulte de la relation précédente que $\alpha\alpha_i$ est divisible par β_1 et que le quotient est un nombre de $I^r . I^{r'}$, donc de I^r, c'est-à-dire $\frac{1}{\beta_1}\alpha\alpha_i = \lambda_i\alpha_1 + \mu_i\alpha_2 + \ldots$, les λ_i, μ_i, etc., entiers ordinaires. On a ainsi, pour $i = 1, 2, \ldots, m$, m relations linéaires et homogènes entre les α_i. Eliminant ces quantités, on a

$$\begin{vmatrix} \lambda_1 - \frac{\alpha}{\beta_1}, & \mu_1, & \ldots \\ \lambda_2, & \mu_2 - \frac{\alpha}{\beta_1}, & \ldots \\ \ldots & \ldots & \ldots \end{vmatrix} = 0,$$

équation à coefficients entiers ordinaires en $\frac{\alpha}{\beta_1}$, d'ordre m, de premier coefficient ± 1. Donc $\frac{\alpha}{\beta_1}$ est un entier (du corps), soit γ, et l'on peut écrire

$$(\gamma) I^r = I^r . I^{r'}.$$

Les nombres $\alpha_1\beta_1, \alpha_2\beta_1, \ldots, \alpha_m\beta_1$ sont des nombres de $I^r I^{r'}$ (car les α_i sont une base de I^r, les β_i de $I^{r'}$); donc, divisés par γ, ce sont des nombres de I^r, c'est-à-dire que

$$\alpha_i \frac{\beta_1}{\gamma} = \lambda_i\alpha_1 + \mu_i\alpha_2 + \ldots \qquad (i = 1, 2, \ldots, m)$$

d'où on conclut encore que $\frac{\beta_1}{\gamma}$, et de même $\frac{\beta_i}{\gamma}$, sont entiers du corps.

Donc $I^{r'} = (\gamma)J$, J étant un nouvel idéal, et $(\gamma)I^r = I^r I^{r'}$ donne $(\gamma)I^r = (\gamma)I^r J$, c'est-à-dire évidemment

$$I^r = I^r J$$

(car ici on peut manifestement diviser par l'idéal *principal* (γ)).

Si δ_1, δ_2, etc., est une base de J, la relation $I^r = I^r J$ montre que α_i est un nombre de $I^r J$; or, un nombre de I^r étant $x_1\alpha_1 + x_2\alpha_2 + \ldots$, un de J étant $y_1\delta_1 + y_2\delta_2 + \ldots$, un nombre de $I^r J$ est manifestement du type $\Sigma\Theta_{j,k}\alpha_j\delta_k$, les $\Theta_{j,k}$ étant entiers du corps.

On a ainsi :

$$\alpha_1 = \alpha_1\Sigma\lambda_i\delta_i + \alpha_2\Sigma\mu_i\delta_i + \ldots + \alpha_m\Sigma\rho_i\delta_i,$$
$$\alpha_2 = \alpha_1\Sigma\lambda'_i\delta_i + \alpha_2\Sigma\mu'_i\delta_i + \ldots + \alpha_m\Sigma\rho'_i\delta_i,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

les λ_i, μ_i, ..., λ'_i, μ'_i, etc., étant entiers du corps. Eliminant les α_i entre ces m relations linéaires et homogènes, il vient

$$\begin{vmatrix} -1 + \Sigma\lambda_i\delta_i, & \Sigma\mu_i\delta_i, & \ldots \\ \Sigma\lambda'_i\delta_i, & -1 + \Sigma\mu'_i\delta_i, & \ldots \\ \ldots & \ldots & \ldots \end{vmatrix} = 0;$$

d'où $\pm 1 =$ polynôme entier par rapport aux δ_i à coefficients entiers du corps, *sans terme indépendant.* Or, les δ_i étant des entiers de J, il en est de même de tout polynôme en δ_i à coefficients entiers quelconques du corps et *sans terme indépendant*, d'après la définition même d'un idéal; donc ± 1 est de J, c'est-à-dire 1 est de J et $J = 1$. L'égalité $I^h = (\gamma)J$ donne donc

$$I^h = (\gamma). \qquad \text{C. q. f. d.}$$

Théorème. — *Cela s'écrit* $I.I^{h-1} = (\gamma)$, *c'est-à-dire que tout idéal multiplié par un autre idéal convenable donne un idéal principal.*

C'est le théorème fondamental d'où se déduit la décomposition unique en idéaux premiers, comme on l'a vu au paragraphe 5.

NOTE III (annexe au § 17),

Par G. HUMBERT.

Démonstration des inégalités fondamentales de Minkowski pour n formes linéaires à n variables.

Il existe trois démonstrations différentes du théorème de Minkowski, énoncé dans le paragraphe 17 sous les deux formes équivalentes des lemmes 6 et 7 : la première, celle de Minkowski, se trouve dans la *Geometrie der Zahlen;* une autre, de M. Hilbert, a été reprise par Minkowski dans ses *Diophantische Approximationen;* on la trouvera aussi dans les *Vorlesungen über Zahlentheorie*, de M. Sommer, traduction française de M. A. Lévy; une troisième a été donnée par M. Hurwitz dans les *Göttinger Nachrichten*, Math.-phys. kl. 1897 : c'est celle qui va être exposée.

Les raisonnements restant les mêmes quel que soit le nombre des variables, on le supposera, pour fixer les idées, égal à trois.

Soient les trois formes linéaires

$$f_i = a_i x + b_i y + c_i z$$

de déterminant Δ. En divisant les a_i, b_i, c_i par $\sqrt[3]{|\Delta|}$, on ramène le déterminant à ± 1, si c'est -1, on changera les signes de a_1, b_1, c_1, et on aura, dans tous les cas,

trois formes f_i' de déterminant ± 1. Dire qu'on peut donner à x, y, z des valeurs entières non toutes nulles, telles que l'on ait

$$|f_i'| \leq 1$$

revient donc à dire que, pour ces valeurs, on a

$$|f_i| \leq \sqrt[3]{\Delta}$$

$\left(\sqrt[n]{\Delta}\right.$ dans le cas de n formes à n variables$\left.\right)$.

C'est sous cette dernière forme que M. Hurwitz établit la proposition.

Sa démonstration se divise en quatre parties.

Première partie. — On supposera d'abord les coefficients des f_i entiers.

Réduction du système des f_i. — On opérera sur x, y, z une suite de substitutions à coefficients entiers de déterminant ± 1, de manière à simplifier les f_i.

Soit $f_1 = a_1 x + b_1 y + c_1 z$; si c_1 est le plus petit (non nul) en valeur absolue des coefficients a_1, b_1, c_1, on peut faire en sorte que le coefficient de x soit, en valeur absolue, inférieur ou au plus égal à $|c_1|$: il suffit d'opérer la substitution $(z, z - \lambda x)$, λ entier; le coefficient de x devient $a_1 - \lambda c_1$ et peut, dès lors, par choix de λ, être > 0 et $\leqslant |c_1|$; ceux de y et de z n'ont pas varié. Si $|a_1|$ est $< |b_1|$ et $|c_1|$, on changera, s'il y a lieu, x en $-x$. On peut donc supposer le coefficient de x positif et non nul, inférieur en valeur absolue à ceux de y et z.

Faisons maintenant la substitution $(x, x + \lambda y)$: nous pouvons rendre le coefficient de y positif ou nul et $< a_1$; puis, par $(y, y + \lambda x)$, diminuer de nouveau celui de x en le laissant toujours positif et non nul; puis, par $(x, x + \lambda y)$, diminuer de nouveau celui de y en le laissant positif ou nul, etc. On arrive ainsi à annuler le coefficient de y et de même celui de z.

f_1 se réduit ainsi à $\mathrm{A}x$, A entier et positif. Opérant de même sur f_2 et y, on peut, par des substitutions opérées successivement sur y et z, faire disparaître le terme en z, en sorte que $f_2 = b'x + \mathrm{B}y$, $\mathrm{B} > 0$. Faisant $(y, y + \lambda x)$, on a

$$f_2 = bx + \mathrm{B}y, \quad \text{avec} \quad 0 \leqslant b < \mathrm{B}, \quad \mathrm{B} > 0.$$

Et alors $f_3 = c'x + c''y + \mathrm{C}z$, où C est $\neq 0$, à cause du déterminant qui est resté le même et est ABC. Par $(z, z + \lambda x)$ et $(z, z + \mu y)$, on peut faire en sorte que l'on ait $0 \leqslant c' < |\mathrm{C}|$, $0 \leqslant c'' < |\mathrm{C}|$.

Finalement, le système est

$$\begin{aligned} f_1 &= \mathrm{A}x, & \mathrm{A} &> 0, \\ f_2 &= bx + \mathrm{B}y, & \mathrm{B} &> 0, \quad 0 \leqslant b < \mathrm{B}, \\ f_3 &= c_1 x + c_2 y + \mathrm{C}z, & 0 &\leqslant (c_1, c_2) < |\mathrm{C}|. \end{aligned}$$

Et les substitutions opérées étant de déterminant ± 1, les anciennes variables sont entières en même temps que les nouvelles et réciproquement.

Pour établir le théorème de Minkowski dans le cas où les f_i ont leurs coefficients entiers, il suffira donc de l'établir pour le système réduit. On peut le faire directement, mais c'est compliqué à cause des cas et sous-cas à distinguer. Mieux vaut raisonner autrement.

Deuxième partie. — Disons que deux formes linéaires et homogènes en x, y, z à coefficients entiers sont *équivalentes* ou *congrues* (modd f_i) si leur différence est du type $\lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, les λ entiers.

Si φ est une telle forme, les $\varphi + \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, sont donc congrues à φ (modd f_i).

Soit $\psi = \varphi + \lambda_1 f_1 + \lambda_2 f_2 + \lambda_3 f_3$, φ étant donnée ; on peut choisir les λ_i de manière que, dans ψ (on dira que ψ est réduite) :

1° Le coefficient de z (qui est celui de z dans φ, augmenté de $C\lambda_3$), soit compris entre o inclus et $|C|$ exclus ;

2° λ_3 étant ainsi déterminé, on peut choisir λ_2, de manière que le coefficient de y soit entre o inclus et B exclus ;

3° Choisir λ_1, de manière que le coefficient de x soit entre o inclus et A exclus.

Alors *les formes ψ réduites sont au nombre de* $|C|BA$ *distinctes*. $|C|BA$ est Δ, déterminant des f_i, et, d'après le calcul précédent, toute forme équivaut (modd f_i) *à une et une seule réduite*. Donc *il y a* $|\Delta|$ *formes et* $|\Delta|$ *seulement non congrues deux à deux, modd* f_i ; parmi elles, celle dont les trois coefficients sont nuls.

Ce résultat obtenu par la réduction des f_i est évidemment vrai pour des f_i non réduites, puisque deux formes congrues (modd f_i) le restent si on opère sur les x, y, z une substitution de déterminant ± 1.

Reprenons alors les f_i initiales. Le théorème du nombre des classes de formes linéaires modd f_i s'applique dès lors aux formes de déterminant Δ :

$$F_1 = a_1 x + a_2 y + a_3 z,$$
$$F_2 = b_1 x + b_2 y + b_3 z,$$
$$F_3 = c_1 x + c_2 y + c_3 z.$$

Soient r^3 et $(r+1)^3$ les cubes positifs d'entiers consécutifs qui comprennent $|\Delta|$, de sorte que $r^3 \leqslant |\Delta| < (r+1)^3$; considérons les formes $\varphi = l_1 x + l_2 y + l_3 z$, où l'on a $0 \leqslant (l_1, l_2, l_3) \leqslant r$. Elles sont $(r+1)^3$, y compris la forme nulle. Comme $(r+1)^3 > |\Delta|$, deux des φ sont congrues entre elles modd F_i, leur différence est donc $\lambda_1 F_1 + \lambda_2 F_2 + \lambda_3 F_3$, les λ n'étant pas nuls à la fois, car les deux φ sont distinctes. On a donc pour des valeurs des l_i entières non nulles à la fois, — car les deux φ sont distinctes, — et comprises entre $-r$ et $+r$ inclus :

$$\lambda_1(a_1 x + a_2 y + a_3 z) + \lambda_2(b_1 x + \ldots) + \lambda_3(c_1 x + \ldots) = l_1 x + l_2 y + l_3 z.$$

d'où

$$a_1\lambda_1 + b_1\lambda_2 + c_1\lambda_3 = l_1,$$
$$a_2\lambda_1 + b_2\lambda_2 + c_2\lambda_3 = l_2,$$
$$a_3\lambda_1 + b_3\lambda_2 + c_3\lambda_3 = l_3,$$

les $|l_i|$ *étant* $\leqslant r$, *c'est-à-dire* $\leqslant |\Delta|^{\frac{1}{3}}$ *et les* λ_i *non nuls à la fois.* Le théorème de Minkowski est donc démontré pour des f_i à coefficients entiers.

Troisième partie. — Il est vrai pour des f_i à coefficients fractionnaires, car si S est le dénominateur commun des coefficients, posons $f_i = \frac{F_i}{S}$, le déterminant des F_i est $S^3\Delta$. Le théorème étant vrai pour les F_i (dont les coefficients sont entiers), on peut trouver x, y, z entiers de telle sorte que $|F_i| \leqslant S|\Delta|^{\frac{1}{3}}$; donc, pour ces valeurs de x, y, z, on a $|f_i| \leqslant |\Delta|^{\frac{1}{3}}$. C. q. f. d.

Quatrième partie. — Soient les f_i à coefficients quelconques et de déterminant $+1$. Nous allons obtenir la démonstration en suivant maintenant un procédé d'Hilbert, qui consiste à comparer les formes f_i à des formes φ_i à coefficients rationnels, suffisamment voisins des premiers. [Voir, par exemple, Sommer.] Soient

$$f_i = a_i x + b_i y + c_i z, \qquad (i = 1, 2, 3)$$

Je dis qu'étant donné un nombre positif δ aussi petit que l'on voudra, il est possible de trouver un nombre ε positif et inférieur à δ, tel que, en faisant varier tous les coefficients, sauf un, de quantités inférieures ou égales à ε en valeur absolue, on n'aura à faire varier le dernier en valeur absolue que de moins de δ pour que le déterminant des formes reste égal à $+1$.

En effet, ce déterminant n'étant pas nul, l'un au moins de ses mineurs d'ordre deux n'est pas nul, soit, par exemple, $a_1 b_2 - a_2 b_1 \neq 0$. Soient α_i, β_i, γ_i les quantités dont nous faisons varier a_i, b_i, c_i. En écrivant que le déterminant reste égal à 1, on a

$$\gamma_3[(a_1+\alpha_1)(b_2+\beta_2) - (a_2+\alpha_2)(b_1+\beta_1)] = \Sigma\alpha_i A_i,$$

le second membre contenant toutes les variations α_i, β_i, γ_i, sauf γ_3 et les A_i, B_i, C_i dépendant des a_i, b_i, c_i et de leurs variations (sauf toujours γ_3). Il est clair qu'en prenant pour la plus grande valeur absolue de ces variations (sauf γ_3) un nombre ε suffisamment petit, on aura $|\gamma_3| < \varepsilon K$, K étant un nombre positif ne dépendant que des a_i, b_i, c_i. Ecrivant $\varepsilon K < \delta$, c'est-à-dire $\varepsilon < \frac{\delta}{K}$, on voit que les variations (sauf γ_3) restant inférieures à ε, $|\gamma_3|$ restera inférieur à δ, et on peut supposer $\varepsilon < \delta$, parce que si $\frac{\delta}{K} > \delta$, on ne prendra que les valeurs de ε inférieures à δ, lesquelles conviennent *a fortiori*.

Faisons de plus les modifications de manière à rendre rationnels tous les coefficients, sauf c_3, et modifions c_3 de manière que le déterminant reste $+1$: c_3 deviendra rationnel par le fait même que les autres coefficients le sont, ainsi que le déterminant. On aura alors trois formes $\varphi_1, \varphi_2, \varphi_3$, dont les coefficients diffèrent de moins de δ de ceux des f_1, f_2, f_3, et telles, d'après la troisième partie, que pour des valeurs des x, y, z, non nulles à la fois, on ait $|\varphi_i| \leqslant 1$, $(i = 1, 2, 3)$.

Observons maintenant que les systèmes de valeurs entières des x, y, z, qui peuvent rendre les $|f_i| \leqslant 1$, sont en nombre limité. Car si l'on pose $f_i = w_i$, $(i = 1, 2, 3)$, les w_i étant compris entre -1 et $+1$, et si on résout ce système en x, y, z, on trouve des fonctions linéaires et homogènes des w_i dont les coefficients dépendent des a_i, b_i, c_i. Donc, les $|w_i|$ étant $\leqslant 1$, les x, y, z sont en valeur absolue inférieurs ou égaux à une limite finie G : les systèmes des x, y, z entiers sont donc en nombre limité.

De même si les φ_i se déduisent des f_i par des variations des coefficients inférieures à δ (le déterminant étant $+1$, comme celui des f_i), on trouve que les systèmes des x, y, z entiers, rendant les $|\varphi_i| \leqslant 1$, sont tels que les x, y, z soient en valeur absolue inférieurs ou égaux à une limite G′ voisine de G.

Considérons les f_i et tous les systèmes de trois formes de déterminant $+1$ qui s'en déduisent par des variations des coefficients inférieures en valeur absolue à δ, et soit G_0 un nombre tel que les x, y, z, qui peuvent rendre un quelconque de ces systèmes $\leqslant 1$ en valeur absolue, soient inférieurs à G_0 en valeur absolue.

Je dis que parmi les systèmes des x, y, z entiers, tels que $(x, y, z) \leqslant G_0$, il en est pour lesquels les $|f_i|$ sont $\leqslant 1$.

Supposons qu'il n'y en ait aucun, c'est-à-dire que pour chaque système considéré il y ait au moins une f_K telle que $|f_K| = 1 + \lambda$, $(\lambda > 0)$, K pouvant varier $(K = 1, 2, 3)$ d'un système à l'autre. Soit λ_0 le plus petit des λ.

La différence entre f_i et φ_i pour un même système de valeurs des variables considérées (c'est-à-dire inférieures ou égales à G_0 en valeur absolue) est inférieure en valeur absolue à $3\delta G_0$; si donc on choisit δ de telle sorte que $3\delta G_0 < \lambda_0$, la valeur de φ_K différera de celle de f_K de moins de λ_0, et comme $|f_K| = 1 + \lambda \geqslant 1 + \lambda_0$, $|\varphi_K|$ sera > 1.

Donc, si, pour chacun des systèmes x_i considérés, un au moins des $|f_i|$ est > 1, on pourra choisir δ de manière que l'un des $|\varphi_i|$ soit également > 1 : c'est en contradiction avec ce qui précède, car on a vu qu'on pouvait faire varier les coefficients des f_i de moins de δ de telle façon que, pour un système de x, y, z au moins, les $|\varphi_i|$ soient $\leqslant 1$. Donc, il faut conclure que, pour un système x_i, au moins les trois f_i sont $\leqslant 1$.

C. q. f. d.

NOTE IV (ANNEXE AU § 59).

PAR G. HUMBERT.

Questions diverses concernant les bases des idéaux d'un corps quadratique.

En raison des fréquentes applications des corps quadratiques, il ne paraîtra pas inutile de rappeler ici les principaux résultats classiques relatifs aux bases des idéaux de ces corps. C'est d'ailleurs une occasion de montrer, dans un cas particulier, la façon d'utiliser les principes généraux du paragraphe 4.

THÉORÈME. — Un idéal quelconque du corps $k(\sqrt{m})$ est un module de ce corps, *déduit de deux nombres fondamentaux*, c'est-à-dire que l'on peut trouver deux entiers du corps e_1 et e_2, tels que tout nombre de l'idéal soit du type $l_1 e_1 + l_2 e_2$, l_1 et l_2 étant des entiers ordinaires et *réciproquement*.

En effet, soient $a + b\omega$, $a_1 + b_1\omega$ deux entiers de l'idéal I (1); l'entier $x(a + b\omega) + y(a_1 + b_1\omega)$, où x et y sont entiers ordinaires, appartient à I. On peut déterminer x et y de manière que $bx + b_1 y$ soit le plus grand commun diviseur de b et b_1, soit b'.

Si $a_2 + b_2\omega$ est un autre nombre de I, il y a de même dans I un nombre où le coefficient de ω est le plus grand diviseur de b' et de b_2, et ainsi de suite.

On arrive ainsi à un nombre $A + h\omega$, où h est le plus grand commun diviseur (positif si l'on veut, car $-A - h\omega$ appartient aussi à I, comme produit d'un nombre de I par -1) de tous les nombres $b, b_1, b_2, \ldots$.

Maintenant $\frac{b}{h}, \frac{b'}{h}, \ldots$, étant entiers, les nombres tels que $a + b\omega - \frac{b}{h}(A + h\omega)$, c'est-à-dire $a - \frac{b}{h}A$, qui sont entiers ordinaires (puisque $\frac{b}{h}$ l'est), appartiennent à I.

I renferme donc les entiers ordinaires en nombre infini : $a - \frac{b}{h}A$; $a_1 - \frac{b_1}{h}A$; ... . (Que I renferme un nombre infini d'entiers ordinaires, c'est évident, car si α est de I, son conjugué α' appartenant au corps, le produit $\alpha'\alpha$, qui est entier ordinaire, est de I.)

Soit q le plus grand commun diviseur positif des nombres entiers ordinaires ci-dessus : $a - \frac{b}{h}A$, etc., de I : il est clair que q appartient à I.

---

(1) On désigne par ω, selon la notation du paragraphe 59, un nombre qui forme avec 1 une base du corps $k(\sqrt{m})$.

Alors un nombre quelconque $a + b\omega$ de I s'écrit :

$$a + b\omega = \frac{b}{h}(\mathrm{A} + h\omega) + \frac{a - \frac{b}{h}\mathrm{A}}{q}\cdot q,$$
$$= x(\mathrm{A} + h\omega) + y\cdot q,$$

x et y étant des entiers ordinaires, puisque h est le plus grand commun diviseur des b et q celui des $a - \frac{b}{h}\mathrm{A}$.

Réciproquement, tout nombre $x(\mathrm{A} + h\omega) + y\cdot q$, où x, y sont entiers ordinaires, appartient à I ; car q et $\mathrm{A} + h\omega$ lui appartiennent.

Donc, I est le *module* de BASE $\mathrm{A} + h\omega$ et q.

On peut simplifier en prenant pour base q et $\mathrm{A} + h\omega + \theta q$ (θ étant un entier ordinaire quelconque), et choisissant θ de manière que l'on ait

$$0 \leqslant \mathrm{A} + \theta q < q.$$

On a ainsi la base q et $g + h\omega$, où q et h sont positifs (*non nuls, comme plus grands communs diviseurs d'entiers ordinaires*) et où l'on a

$$0 \leqslant g < q.$$

Réciproque. — Le module de base q et $g + h\omega$ est-il un idéal ?

Pour cela, il faut et il suffit que

$$q(x + y\omega) + (g + h\omega)(z + t\omega),$$

où x, y, z, t sont entiers ordinaires quelconques, appartienne au module. Comme la somme de deux nombres du module lui appartient aussi, il faut et il suffit que q, $q\omega$, $g + h\omega$, $\omega(g + h\omega)$ appartiennent au module ; q et $g + h\omega$ lui appartiennent. Pour que $q\omega$ lui appartienne aussi, il faut

$$q\omega = xq + y(g + h\omega) ;$$

d'où

$$q = yh, \qquad 0 = xq + yg.$$

Donc : 1° *h divise q* ; $q = hq_1$ et, par suite, $y = q_1$; et $xq = -yg$ donne alors $xhq_1 = -q_1 g$ ou $xh = -g$; d'où, 2° *h divise g* : $g = hg_1$.

Enfin, pour que $\omega(g + h\omega)$ appartienne au module, il faut

$$\omega(g + h\omega) = xq + y(g + h\omega),$$

ce qui, en distinguant $m \not\equiv 1$ et $m \equiv 1$, mod 4, donne

1° $$m \not\equiv 1, \qquad \omega^2 = m ;$$

d'où

$$g = hy, \qquad hm = xq + yg ;$$

h divisant g, y est un entier g_1; ensuite $hm = xhq_1 + g_1^2 h$ montre que $\frac{m - g_1^2}{q_1}$ doit être entier.

$$2^\circ \qquad m \equiv 1, \quad \omega^2 - \omega = \frac{m-1}{4};$$

d'où

$$\omega g + h\left(\omega + \frac{m-1}{4}\right) = xq + y(g + h\omega),$$

et

$$g + h = hy, \quad h\frac{m-1}{4} = xq + yg,$$

c'est-à-dire, puisque $g = hg_1$:

$$g_1 + 1 = y, \quad h \cdot \frac{m-1}{4} = xhq_1 + hg_1(g_1 + 1),$$

et donc

$$\frac{1}{q_1}\left[\frac{m-1}{4} - g_1(g_1 + 1)\right]$$

doit être entier.

Donc, pour que le module de base q, $g + h\omega$, soit un idéal, il faut et il suffit que $q = hq_1$; $g = hg_1$ et que

si $m \not\equiv 1$, (mod 4), $g_1^2 - m$ soit multiple de q_1,

si $m \equiv 1$, (mod 4), $g_1^2 + g_1 - \frac{m-1}{4}$ soit multiple de q_1.

Dans tous les cas, m est résidu quadratique de q (et même de $4q_1$, si m est $\equiv 1$, mod 4).

L'idéal $(q, g + h\omega)$ ou $(q_1 h, g_1 h + h\omega)$ a tous ses nombres divisibles par h : il s'écrit évidemment

$$(q, g + h\omega) = (h)(q_1, g_1 + \omega),$$

c'est-à-dire est le produit de l'idéal principal (h) par l'idéal $(q_1, g_1 + \omega)$, dont les nombres ne sont plus divisibles évidemment par un même entier ORDINAIRE.

Ce dernier idéal sera dit *idéal* NORMAL.

BASE CANONIQUE. — Une base de l'idéal I : q, $g + h\omega$ où q et g sont divisibles par h, où q, h sont > 0 et où g est $\geqslant 0$ et $< q$, est dite *base canonique* de cet idéal.

Il n'y a qu'une base canonique.

Car si q', $g' + h'\omega$ en est une autre, on a d'abord $h' = h$, car, d'après ce qui précède, h est le plus grand diviseur commun entier ordinaire de tous les nombres de l'idéal, et de même h'.

Ensuite, tous les entiers ordinaires de I sont q et les multiples entiers ordinaires

de q (par $qx + (g + h\omega)y$), de même ce sont q' et ses multiples; donc $q' = q$, puisque q et q' sont positifs. Enfin, $g' + h\omega$ étant de I, on a : $g' + h\omega = qx + y(g + h\omega)$, d'où $y = 1$, c'est-à-dire $g' = qx + g$, et comme on a

$$0 \leqslant g' < q \quad \text{et} \quad 0 \leqslant g < q,$$

il faut $x = 0$ et $g' = g$. C. q. f. d.

Mais il y a une infinité de *bases non canoniques*, c'est-à-dire de couples $\alpha + \beta\omega$, $\alpha' + \beta'\omega$, tels que tout entier de I soit $x(\alpha + \beta\omega) + y(\alpha' + \beta'\omega)$ avec x, y, entiers ordinaires.

Il suffit en effet de prendre

$$\alpha + \beta\omega = x_1 q + y_1(g + h\omega),$$
$$\alpha' + \beta'\omega = x_2 q + y_2(g + h\omega),$$

x_1, y_1, x_2, y_2 entiers ordinaires tels que l'on ait

$$x_1 y_2 - x_2 y_1 = \pm 1.$$

Alors, q et $g + h\omega$ sont de la forme

$$n(\alpha + \beta\omega) + n'(\alpha' + \beta'\omega),$$

n et n' entiers ordinaires, et tout entier de I étant $q\xi + (g + h\omega)\eta$, ξ et η entiers ordinaires, la proposition est établie. La réciproque est évidente, toute base s'obtient ainsi.

Problème. — Le module de base $\alpha + \beta\omega$, $\alpha' + \beta'\omega$ est-il un idéal?

Il faut chercher dans ce module une base canonique et voir si elle satisfait aux relations voulues pour être base d'idéal. *On va prouver qu'un module a une base canonique et une seule.*

D'abord $\alpha\beta' - \beta\alpha'$ ne peut être nul. Car soit δ le plus grand commun diviseur des entiers ordinaires α et β, δ' celui de α' et β', on a

$$\alpha + \beta\omega = \delta(a + b\omega), \qquad \alpha' + \beta'\omega = \delta'(a' + b'\omega),$$

et on a

$$ab' - ba' = 0, \qquad \text{si} \qquad \alpha\beta' - \beta\alpha' = 0.$$

On en conclut, a et b étant premiers entre eux ainsi que a' et b' :

$$a' = \varepsilon a, \quad b' = \varepsilon b, \quad \varepsilon = \pm 1.$$

Alors on peut écrire

$$\alpha + \beta\omega = \delta(a + b\omega), \qquad \alpha' + \beta'\omega = \delta_1(a + b\omega).$$

On peut supposer δ et δ_1 premiers entre eux, en faisant au besoin rentrer leur plus grand commun diviseur dans $a + b\omega$. Alors $a + b\omega$ est un nombre du module, qui ne comprend dès lors que les multiples entiers ordinaires de $a + b\omega$. Un tel module ne peut être un idéal, car celui-ci, comprenant $a + b\omega$, comprendrait aussi $\omega(a + b\omega)$, et ω n'est pas entier ordinaire.

Cela posé, on aura une base canonique par

$$x(\alpha + \beta\omega) + y(\alpha' + \beta'\omega) = \text{quantité réelle positive } q,$$
$$x'(\alpha + \beta\omega) + y'(\alpha' + \beta'\omega) = g + h\omega, \quad \text{avec } h > 0,$$
$$0 \leqslant g < q,$$
$$xy' - yx' = \pm 1.$$

Cela donne $\beta x + \beta' y = 0$, d'où x et y, puisqu'ils sont premiers entre eux ; quant au signe, il est déterminé par la condition $\alpha x + \alpha' y > 0$.

Ensuite, $xy' - yx' = \pm 1$ donne

$$x' = \varepsilon(x_0' + \theta x), \quad y' = \varepsilon(y_0' + \theta y), \quad \varepsilon = \pm 1,$$

θ entier ordinaire quelconque, x_0', y_0' solution particulière. Alors, $\beta x' + \beta' y' > 0$ donne, puisque $\beta x + \beta' y = 0$,

$$\varepsilon(\beta x_0' + \beta' y_0') > 0,$$

d'où le signe de ε. Et enfin

$$0 \leqslant \varepsilon[\alpha(x_0' + \theta x) + \alpha'(y_0' + \theta y)] < q$$

ou

$$0 \leqslant \varepsilon(M + \theta q) < q \qquad (\text{car } \alpha x + \alpha' y = q)$$

donne θ sans ambiguïté.

On trouve ainsi une et une seule base canonique pour le module considéré.

NOTE V (ANNEXE AU § 118),

PAR TH. GOT.

Détail de la démonstration de la seconde expression du nombre de classes d'idéaux du corps circulaire des racines $l^{\text{ièmes}}$ de l'unité, l étant premier.

On part de la première expression, transformée à l'aide de l'identité d'Euler :

$$\varkappa h = \prod_{(u)} \operatorname*{Lim}_{s=1} \prod_{(p)} \left(1 - \left[\frac{p}{l}\right]^u p^{-s}\right)^{-1} = \prod_{(u)} \operatorname*{Lim}_{s=1} \sum \left[\frac{n}{l}\right]^u \frac{1}{n^s}$$
$$(u = 1, 2, \ldots, l-2)$$

On a, pour n non divisible par l :

$$\left[\frac{n}{l}\right] = e^{\frac{2i\pi}{l-1}}.$$

ν désignant l'indice de n par rapport au module l et à une racine primitive $r (r^\nu \equiv n, \bmod l)$; et, pour n divisible par l, on pose :

$$\left[\frac{n}{l}\right] = 0.$$

Si $n' \equiv n, (l)$, on a $\nu' \equiv \nu, (l-1)$; donc

$$\left[\frac{n'}{l}\right] = \left[\frac{n}{l}\right],$$

et l'on a, par suite,

$$\Sigma = \sum_{k=1}^{k=l-1} \left[\frac{k}{l}\right]^u \left(\frac{1}{k^s} + \frac{1}{(k+l)^s} + \frac{1}{(k+2l)^s} + \dots\right).$$

Mais

$$\frac{1}{n^s} = \frac{1}{\Gamma(s)} \int_0^\infty e^{-nt} t^{s-1} dt$$

$$\frac{1}{k^s} + \frac{1}{(k+l)^s} + \dots = \frac{1}{\Gamma(s)} \int_0^\infty t^{s-1} dt (e^{-kt} + e^{-(k+l)t} + \dots) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{e^{-kt}}{1-e^{-lt}} t^{s-1} dt.$$

Donc, comme $\Gamma(1) = 1$,

$$\chi h = \prod_u \lim_{s=1} \int_0^\infty \frac{t^{s-1} dt}{1-e^{-lt}} \sum_{n=1}^{n=l-1} e^{-nt} e^{\frac{2i\pi u\nu}{l-1}}.$$

Posons

$$F_u(e^{-t}) = \sum_{n=1}^{n=l-1} e^{-nt} e^{\frac{2i\pi u\nu}{l-1}},$$

$$\chi h = \prod_u \lim_{s=1} \int_0^\infty \frac{t^{s-1} F_u(e^{-t})}{1-e^{-lt}} dt.$$

$F_u(e^{-t}) = 0$ pour $t = 0$, car $\sum_{\nu=1}^{\nu=l-1} e^{\frac{2i\pi u\nu}{l-1}} = 0$. Donc, $F_u(e^{-t})$ est divisible par $1 - e^{-t}$, comme $1 - e^{-lt}$, et la fraction $\frac{F_u(e^{-t})}{1-e^{-lt}}$ reste finie pour $t = 0$; on a donc :

$$\lim_{s=1} \int_0^\infty \frac{F_u(e^{-t}) t^{s-1} dt}{1-e^{-lt}} = \int_0^\infty \frac{F_u(e^{-t}) dt}{1-e^{-lt}}.$$

Posons $e^{-t} = x$, $e^{-t} dt = -dx$. L'intégrale devient

$$\int_0^1 \frac{F_u(x) dx}{x(1-x^l)}.$$

En décomposant en fractions simples, on a :

$$\frac{F_u(x)}{x(1-x^l)} = -\frac{1}{l}\sum_{q=1}^{l-1}\frac{F_u\left(e^{\frac{2qi\pi}{l}}\right)}{x - e^{\frac{2qi\pi}{l}}},$$

$$F_u\left(e^{\frac{2qi\pi}{l}}\right) = \sum_{k=1}^{k=l-1}\zeta^{qk}\theta^{u\,\mathrm{ind}\,k}$$

en posant $\theta = e^{\frac{2i\pi}{l-1}}$.

Soit u impair. — On a :

$$F_u\left(e^{\frac{2qi\pi}{l}}\right) = \theta^{-u\,\mathrm{ind}\,q}F_u\left(e^{\frac{2i\pi}{l}}\right).$$

D'ailleurs,

$$\int_0^1 \frac{dx}{x - e^{\frac{2qi\pi}{l}}} = L\left(2\sin\frac{q\pi}{l}\right) + \frac{\pi}{2}\left(1 - \frac{2q}{l}\right)i,$$

L désignant la partie réelle du logarithme.

Pour deux valeurs q, q' complémentaires à l, le L a même valeur, et

$$\mathrm{ind}\,q' = \mathrm{ind}\,q + \frac{l-1}{2}, \qquad \theta^{-u\,\mathrm{ind}\,q'} = -\theta^{-u\,\mathrm{ind}\,q},$$

car u est impair.

Les termes logarithmiques se détruisent donc dans la somme.

Puis $$\frac{\pi}{2}\sum\theta^{-u\,\mathrm{ind}\,q} = 0, \quad \text{car} \quad u \not\equiv 0, \pmod{l-1}.$$

Reste $$-\frac{\pi i}{l}\sum q\,\theta^{-u\,\mathrm{ind}\,q};$$

et par suite le produit relatif aux valeurs impaires de u se réduit à

$$\left(\frac{\pi i}{l^2}\right)^{\frac{l-1}{2}}\prod_u F_u\left(e^{\frac{2i\pi}{l}}\right)\prod_{u=1,3,\ldots,l-2}\sum q\,\theta^{u\,\mathrm{ind}\,q}.$$

(On a changé θ en θ^{-1} dans le second produit, ce qui est permis, les valeurs de u étant deux à deux complémentaires à $l-1$.)

Quant au premier produit $\prod_u F_u\left(e^{\frac{2i\pi}{l}}\right)$, on remarque que, d'après des formules de la division du cercle,

$$F_u\left(e^{\frac{2i\pi}{l}}\right) \times F_{l-1-u}\left(e^{\frac{2i\pi}{l}}\right) = \pm l,$$

suivant que u est pair ou impair, et que

$$F_{\frac{l-1}{2}}\left(e^{\frac{2i\pi}{l}}\right) = \pm\sqrt{\pm l}.$$

Donc $$\prod_{u=1}^{u=l-2} F_u\left(e^{\frac{2i\pi}{l}}\right) = \pm i\,l^{\frac{l-2}{2}}.$$

Soit u pair. — Les termes non logarithmiques se détruisent. En posant

$$\mathrm{L}\Lambda_q = \mathrm{L}\sqrt{\left(1 - e^{\frac{2qi\pi}{l}}\right)\left(1 - e^{-\frac{2qi\pi}{l}}\right)} = \mathrm{L}\, 2 \sin\frac{q\pi}{l},$$

le produit étendu aux $\frac{l-3}{2}$ valeurs paires de u, s'écrit

$$\frac{1}{l^{\frac{l-3}{2}}} \prod_{u=2,4,\ldots,l-3} \Sigma\, \theta^{-u \,\mathrm{ind}\, q}\, \mathrm{L}\Lambda_q,$$

à i^2 près (q ne prenant plus dans la somme que les valeurs inférieures à $\frac{l}{2}$).

Donc, puisque

$$\chi = \frac{2^{r_1+r_2}\pi^{r_2}\mathrm{R}}{w\left|\sqrt{d}\right|}$$

est ici

$$\frac{(2\pi)^{\frac{l-1}{2}}\mathrm{R}}{2l \times l^{\frac{l-2}{2}}}$$

on a

$$\frac{(2\pi)^{\frac{l-1}{2}}\mathrm{R}h}{2l^{\frac{l}{2}}} = \pm i \frac{l^{\frac{l-2}{2}}}{l^{\frac{l-3}{2}}} \left(\frac{\pi}{l^2}\right)^{\frac{l-1}{2}} \prod_{u=1,3,\ldots,l-2} \Sigma_q\, q\, \theta^{u \,\mathrm{ind}\, q} \prod_{u=2,4,\ldots,l-3} \Sigma\, \theta^{-u \,\mathrm{ind}\, q}\, \mathrm{L}\Lambda_q,$$

$$h = \frac{1}{(2l)^{\frac{l-3}{2}}\mathrm{R}}\, \Pi_1 \Pi_2,$$

en désignant par Π_1 et Π_2, pour abréger les deux produits du second membre.

Enfin, pour obtenir la forme plus simple du théorème 142 :

$$h = \frac{\Pi_1}{(2l)^{\frac{l-3}{2}}} \frac{\Delta}{\mathrm{R}},$$

remarquons qu'en changeant un peu les notations et posant

$$\Lambda_q = \sqrt{(1 - \zeta^{r^q})(1 - \zeta^{-r^q})},$$

on a $\varepsilon_q = \frac{\Lambda_q}{\Lambda_{q-1}}$, et, par suite, $\log \varepsilon_q = \mathrm{L}\Lambda_q - \mathrm{L}\Lambda_{q-1}$, et l'on trouve alors

$$\sum_u \theta^{-uq}\, \mathrm{L}\Lambda_q (1 - \theta^{-u}) = \log \varepsilon_1 + \theta^u \log \varepsilon_2 + \ldots + \theta^{\frac{l-3}{2}u} \log \varepsilon_{\frac{l-1}{2}}.$$

Comme

$$\prod_{u=2,4,\ldots,l-3} (1 - \theta^{-u}) = \frac{l-1}{2},$$

et que

$$\Pi\, \Sigma\, \theta^{ku} \log \varepsilon_{k+1} = \frac{l-1}{2} \Delta,$$

la formule est démontrée.

NOTE VI (ANNEXE AU § 172).

Par Th. GOT.

Recherches sur le théorème de Fermat, faites par Kummer et divers auteurs, postérieurement à la démonstration de l'impossibilité en nombres entiers de l'équation

(1) $$x^l + y^l + z^l = 0,$$

donnée par Kummer pour les exposants *l* premiers réguliers.

La fondation récente du prix Wolfskehl a donné un renouveau d'actualité à la question du théorème de Fermat et a suscité un grand nombre de travaux s'y rapportant. Il nous a paru intéressant d'indiquer l'état de la question à la fin de 1911. Mais pour comprendre la portée des travaux actuels et même les méthodes qui ont inspiré certains d'entre eux, il est indispensable de se reporter aux résultats obtenus déjà par Kummer il y a cinquante ou soixante ans : il a d'abord démontré l'impossibilité de l'équation de Fermat pour les exposants l premiers réguliers (c'est-à-dire ne divisant le numérateur d'aucun des $\frac{l-3}{2}$ premiers nombres de Bernoulli) : c'est à ce théorème que le dernier chapitre du Rapport de M. Hilbert est consacré; Kummer a ensuite, dans un Mémoire de 1857 (*Abhandlungen der Königl. Akad. der Wissenschaften zu Berlin*), étendu la démonstration à la classe particulière suivante d'exposants l premiers non réguliers :

1° l divise un seul, B_ν, des $\frac{l-3}{2}$ premiers nombres de Bernoulli et une seule fois;

2° il existe un module pour lequel une certaine unité E_ν n'est pas reste de $l^{\text{ième}}$ puissance;

3° $B_{\nu l}$ n'est pas divisible par l^3.

C'est à l'exposé de ce résultat que la plus grande partie de la présente note est consacrée : tout en suivant la marche de Kummer, j'ai apporté à ses démonstrations les changements nécessaires pour les faire cadrer avec la conception actuelle des idéaux (d'après la définition de Dedekind) et avec les procédés et les notations du Rapport de M. Hilbert. A part deux exceptions relatives à des questions très simples, pour lesquelles je renvoie le lecteur aux Mémoires de Kummer, je me suis

d'ailleurs astreint à réunir dans ma Note, lorsqu'elles ne se trouvaient pas déjà dans le Rapport, les démonstrations de toutes les propositions utilisées : on n'aura pas ainsi à les chercher dans plusieurs longs Mémoires de Kummer où elles sont disséminées; j'ai, du reste, pu, sur quelques points, abréger notablement les calculs, soit en traitant d'une manière unique les cas des idéaux premiers du premier degré et de ceux de degré quelconque, soit en utilisant les résultats du Rapport. Exception faite des deux exceptions mentionnées, la lecture de notre Note n'exige donc, en dehors de l'étude de ce Rapport, aucune étude supplémentaire. J'ai conservé, pour les renvois aux théorèmes ou paragraphes, et pour les références bibliographiques, les abréviations de cet Ouvrage, et j'ai distingué par des chiffres romains les divisions et les théorèmes de la Note.

Parmi les travaux récents, nous nous contenterons — renvoyant pour les démonstrations aux Mémoires originaux — d'indiquer les plus importants des résultats obtenus, soit en partant de ceux de Kummer [Mirimanoff, Wieferich, Frobenius], soit dans un autre ordre d'idées, voisin de celui de Legendre [Dickson, Hurwitz].

L'étude de l'équation (1) est entièrement différente suivant que l'un des nombres x, y, z est ou n'est pas divisible par l; nous examinerons donc les deux cas successivement.

I. — Étude du cas où xyz n'est pas divisible par l.

§ I. — *Étude d'un produit particulier d'idéaux conjugués.*

Théorème I. — Soit r une racine primitive, module l, et désignons par r_a le plus petit reste positif de r^a, module l, et par s la substitution (ζ, ζ^r). $\mathfrak{j}$ désignant un idéal quelconque, le produit $\prod_k s^k\mathfrak{j}$ est toujours un idéal principal, lorsqu'on l'étend soit aux $\frac{l-1}{2}$ valeurs de k vérifiant l'inégalité

$$(3) \qquad r_{-k} + r_{k+\operatorname{ind} q} < l,$$

soit aux $\frac{l-1}{2}$ valeurs de k vérifiant l'inégalité inverse. q désigne un entier quelconque non divisible par l; l'indice est relatif à la racine primitive r, module l. [Kummer[6]].

Démonstration. — Nous allons démontrer d'abord (lemme I) que le théorème est vrai pour tout idéal premier du premier degré. Nous établirons ensuite (lemme II) que tout idéal premier de degré quelconque est équivalent à un produit d'idéaux premiers du premier degré, ce qui achèvera la démonstration.

Lemme I. — $\mathfrak{p}$ étant un idéal premier du premier degré, le produit $\prod_k s^k\mathfrak{p}$, étendu aux mêmes valeurs de k que ci-dessus, est un idéal principal [1].

Soit, en effet, p le nombre premier rationnel divisible par $\mathfrak{p}$; il est de la forme $ml + 1$, puisque $\mathfrak{p}$ est du premier degré, et il se décompose en $l - 1$ facteurs conjugués :

$$p = \prod_{i=0}^{i=l-2} s^i\mathfrak{p}.$$

D'autre part, on a la formule suivante, de la division du cercle :

$$p = \psi_q(\zeta)\psi_q(\zeta^{-1}),$$

dans laquelle $\psi_q(\zeta)$ désigne la somme

$$\psi_q(\zeta) = \sum_{t=1}^{t=p-2} \zeta^{\operatorname{ind} t + q \operatorname{ind}(t+1)},$$

où les indices sont pris par rapport à une racine primitive g, module p. (Voir, par exemple, Weber, *Algèbre supérieure*.)

Soit, d'autre part,

$$\mathfrak{p} = (p, \zeta - g^m).$$

(Voir note du § 93.)

Cherchons à quelle condition l'idéal

$$s^k\mathfrak{p} = (p, \zeta^{r^k} - g^m)$$

est un diviseur de $\psi_q(\zeta)$. Il faut et il suffit pour cela que la division de $\psi_q(\zeta)$ par $\zeta^{r^k} - g^m$ donne un reste divisible par p. Pour avoir ce reste R, (mod p), nous remplaçons ζ^{r^k} par g^m, c'est-à-dire ζ par $g^{mr^{-k}}$, et nous avons

$$\mathrm{R} = \sum_{t=1}^{t=p-2} g^{mr^{-k}(\operatorname{ind} t + q \operatorname{ind}(t+1))} \equiv \sum_{t=1}^{t=p-2} t^{mr^{-k}}(t+1)^{qmr^{-k}} \equiv \sum_{t=1}^{t=p-1} t^{mr^{-k}}(t+1)^{qmr^{-k}}, \pmod{p},$$

ou encore, en remplaçant mr^{-k} et mqr^{-k} par mr_{-k} et $mr_{-k+\operatorname{ind} q}$, ce qui ne modifie pas les exposants pour le module $ml = p - 1$:

$$\mathrm{R} \equiv \sum_{t=1}^{t=p-1} t^{mr_{-k}}(t+1)^{mr_{-k+\operatorname{ind} q}}.$$

---

[1] Ce lemme est identique au théorème 136, si l'on prend $q = r = 1$; en raison de son importance, nous en donnons une autre démonstration, d'après les procédés de Kummer.

En développant par la formule du binôme, nous aurons

$$R = \sum_u a_u \sum_{t=1}^{t=p-1} t^u,$$

expression dans laquelle les a_u sont des coefficients binômiaux, dont aucun n'est divisible par p, puisque l'on a

$$mr_{-k+\mathrm{ind}\,q} < p - 1.$$

Les sommes $\sum_{t=1}^{t=p-1} t^u$ sont divisibles par p, sauf si t^u est congru à 1, module p, c'est-à-dire, — u étant compris entre zéro et $2p-2$, — si u est égal à $p-1$. La condition nécessaire et suffisante pour que R soit divisible par p, et que, par suite, $s^k\mathfrak{p}$ divise $\psi_q(\zeta)$, est donc que la plus grande valeur de u soit inférieure à $p-1$:

$$mr_{-k} + mr_{-k+\mathrm{ind}\,q} < p - 1,$$

ou, en divisant par m :

$$r_{-k} + r_{-k+\mathrm{ind}\,q} < l.$$

Or, de deux nombres k et $\mu + k$ (1), l'un vérifie l'inégalité ci-dessus et l'autre l'inégalité inverse (car $r_{\mu+k} = l - r_{-k}$); par suite, la moitié des $l-1$ idéaux premiers de p divisent $\psi_q(\zeta)$ et l'autre moitié $\psi_q(\zeta^{-1})$, — comme on le voit d'ailleurs *a priori* en changeant ζ en ζ^{-1}; — et comme $\psi_q(\zeta)\psi_q(\zeta^{-1})$, qui est égal à p, ne contient que $l-1$ facteurs idéaux, on a nécessairement (2)

$$\prod_k s^k\mathfrak{p} = \pm\zeta^u\psi_q(\zeta).$$

et

$$\prod_{\mu-k} s^{\mu-k}\mathfrak{p} = \pm\zeta^{-u}\psi_q(\zeta^{-1}),$$

k prenant, dans ces deux produits, les valeurs vérifiant l'inégalité (3) ou l'inégalité équivalente :

(4) $$r_{\mu-k} + r_{\mu-k+\mathrm{ind}\,q} > l.$$

Ces produits sont donc des idéaux principaux. C. q. f. d.

---

(1) $\mu = \frac{l-1}{2}$.

(2) $E(\zeta)$, unité à introduire dans le produit, est nécessairement de la forme $\pm\zeta^u$, car $E(\zeta).E(\zeta)^{-1} = 1$. (Théorème 48.)

Lemme II. — Tout idéal premier $\mathfrak{p}$ de degré quelconque f est équivalent à un produit d'idéaux premiers du premier degré.

Il suffit évidemment de démontrer que tout idéal premier de degré supérieur à 1 est équivalent à un produit d'idéaux premiers de degré inférieur. Nous allons pour cela déterminer un nombre $F(\zeta)$, divisible par $\mathfrak{p}$ une fois et une seule, et dont tous les autres facteurs idéaux premiers $\mathfrak{q}$ soient de degré inférieur. On aura donc

$$F(\zeta) = \mathfrak{p}\Pi\mathfrak{q},$$

et comme la norme de $\Pi\mathfrak{q}$ est un entier N,

$$N = \Pi\mathfrak{q}\,.\,s\Pi\mathfrak{q}\,.\,s^2\Pi\mathfrak{q}\,.\,\dots\,.\,s^{l-2}\Pi\mathfrak{q},$$

on aura ainsi montré l'équivalence de $\mathfrak{p}$ au produit $s\Pi\mathfrak{q}\,.\,s^2\Pi\mathfrak{q},\,\dots\,s^{l-2}\Pi\mathfrak{q}$, dont tous les idéaux sont de degré moindre.

Pour le nombre $F(\zeta)$, il suffit de prendre $P(\zeta)+p$, en désignant par $P(x)$ le facteur correspondant à $\mathfrak{p}$ dans l'équation fondamentale décomposée, module p, en ses $e = \frac{l-1}{f}$ facteurs irréductibles :

$$x^{l-1} + x^{l-2} + \dots + 1 \equiv P(x)\,.\,P_1(x)\dots P_{e-1}(x) \quad (\text{mod } p),$$

de sorte que l'on a

$$\mathfrak{p} = \big(p,\ P(\zeta)\big)$$

(voir théorème 119).

Pour démontrer que $F(\zeta)$ remplit bien les conditions indiquées, remarquons que le premier coefficient de P peut être pris égal à 1 et démontrons que le dernier est alors égal, module p, à $(-1)^f$. Considérons pour cela l'équation

$$\Phi_k(x) = x^f + A_1(\eta_k)x^{f-1} + \dots + A_f(\eta_k) = 0$$

dont les racines sont les racines de l'unité formant la période $\eta_k(\eta_k = \zeta^{r^k} + \zeta^{r^{k+e}} + \dots + \zeta^{r^{k+(f-1)e}})$. Le produit de ces racines de l'unité étant égal à 1, on a

$$A_f(\eta_k) = (-1)^f.$$

Le produit $\prod\limits_{k=0}^{k=e-1} \Phi_k(x)$ est un polynôme à coefficients entiers, — car ces coefficients sont des fonctions symétriques des périodes, — et il est identique au premier membre de l'équation fondamentale, — car il a même degré, mêmes racines et même premier coefficient. Soit, d'autre part,

$$\varphi(y) = 0$$

l'équation de degré e, à coefficients entiers, dont les racines sont les e périodes à f termes : cette équation, considérée comme congruence, module p, a e racines u_k. [Kummer[3].] Faisons correspondre, d'une façon quelconque, ces dernières aux périodes

et substituons dans les Φ_k les u_k aux η_k. Puisque les fonctions symétriques élémentaires des u_k sont congrues, pour le module p, aux mêmes fonctions des périodes, on a la congruence

$$x^{l-1} + x^{l-2} + \ldots + 1 \equiv \prod_{k=0}^{k=e-1} \Phi_k(x, u_k), \qquad (\text{mod } p).$$

Comme le polynôme $x^{l-1} + x^{l-2} + \ldots + 1$ ne peut être décomposé de deux manières différentes en facteurs irréductibles, module p, les $P_j(x)$ ne sont autres, à l'ordre près, que les $\Phi_k(x, u_k)$, ce qui démontre notre assertion sur la valeur du dernier coefficient de $P(x)$.

Dès lors, $P(\zeta) + p$ est :

1° Divisible par $\mathfrak{p}$;

2° Non divisible par $\mathfrak{p}^2$, car tout nombre divisible par $\mathfrak{p}^2$ doit, après division par $P(\zeta)$, donner un reste divisible par p^2, et ici le reste est p ;

3° Non divisible par un autre facteur $\mathfrak{p}_k$ de p, égal à $\big(p, P_k(\zeta)\big)$, car le polynôme $P(x)$ n'est pas divisible par $P_k(x)$, mod p ;

4° Non divisible par un idéal premier de degré supérieur à f, car $P(\zeta)$ est de degré f et le premier coefficient est 1 ;

5° Non divisible par un idéal premier de degré f autre que $\mathfrak{p}$, car, soit $\mathfrak{q}$, égal à $\big(q, Q(\zeta)\big)$, un tel idéal ; le reste de la division de $P(x) + p$ par $Q(x)$ est $P(x) - Q(x) + p$, et il n'est pas divisible par q, puisque les derniers termes de P et Q étant égaux $\big($à $(-1)^f\big)$, le dernier terme du reste est p.

Le nombre $F(\zeta) = P(\zeta) + p$ remplit donc les conditions que nous avons utilisées et le lemme II se trouve ainsi démontré, ce qui achève la démonstration du théorème I [1].

§ II. — *Le critérium de Kummer.*

Théorème II. — Si trois entiers rationnels x, y, z, premiers entre eux et à l, vérifient l'équation

$$x^l + y^l + z^l = 0,$$

chaque couple de deux quelconques d'entre eux, x, y, vérifie le système des $\frac{l-3}{2} = \nu - 1$ congruences suivantes [2] :

$$B_n \frac{d_0^{l-2n} \log (x + e^u y)}{du^{l-2n}} \equiv 0, \qquad (\text{mod } l), \qquad (n = 1, 2, \ldots, \nu - 1) \tag{5}$$

---

[1] Le lemme II est vrai pour un corps de Galois quelconque (théorème 89), il nous a paru utile d'en reproduire la démonstration particulière au corps circulaire.

[2] $\frac{d_0^{l-2n}}{du^{l-2n}}$ désigne la valeur de la dérivée $(l-2n)^{\text{ième}}$ pour $u = 0$.

En effet, l'équation peut s'écrire

$$(x+y)(x+\zeta y)\ldots(x+\zeta^{l-1}y) = -z^l.$$

Les facteurs du premier membre sont premiers entre eux deux à deux, puisque x et y sont premiers entre eux et que z est premier à l (voir § 179) ; donc, leur produit étant une puissance $l^{\text{ième}}$, chacun d'eux est, à un facteur unité près, la puissance $l^{\text{ième}}$ d'un idéal. On a donc

$$x+\zeta y = \varepsilon \mathfrak{j}^l,$$

et, par suite,

$$x+\zeta^{r^k} y = s^k\varepsilon (s^k\mathfrak{j})^l,$$

(s désignant toujours la substitution (ζ, ζ^r)).

Donnons à k les $\frac{l-1}{2}$ valeurs vérifiant l'inégalité (4) :

$$r_{\mu-k} + r_{\mu-k+\operatorname{ind} q} > l,$$

et formons le produit des $x - \zeta^{r^k}y$ étendu à ces valeurs de k ; on sait (théorème I) que le produit $\prod\limits_k s^k\mathfrak{j}$ correspondant est un idéal principal (α). Quant au produit $\prod\limits_k s^k\varepsilon$, il se réduit, au signe près, à une racine $l^{\text{ième}}$ de l'unité (théorème 48), car son module est égal à ± 1, puisque l'on a pour la norme :

$$n(\varepsilon) = \prod_k s^k\varepsilon \cdot \prod_{\mu+k} s^{\mu+k}\varepsilon = \pm 1$$

et que $\prod\limits_k$ et $\prod\limits_{\mu-k}^{k}$ qui se déduisent l'un de l'autre par le changement de ζ en ζ^{-1} sont imaginaires conjugués. On a donc

$$\prod_k (x-\zeta^{r^k}y) = \pm\zeta^t\alpha^l.$$

On en déduit (voir § 131, note), les congruences

(6) $$\sum_k \frac{d_0^{l-2n}\log(x-e^{ur^k}y)}{du^{l-2n}} \equiv 0, \quad (\text{mod } l),$$

pour $n = 1, 2, \ldots, \mu-1$, c'est-à-dire encore

$$\frac{d_0^{l-2n}\log(x-e^{u}y)}{du^{l-2n}} \sum_k r^{k(l-2n)} \equiv 0, \quad (\text{mod } l).$$

Transformons $\sum\limits_k$, de manière à étendre la sommation à toutes les valeurs de k de 1 à $l-1$, en multipliant chaque terme de $\sum\limits_{k=1}^{k=l-1} r^{k(l-2n)}$ par la fraction

$$\frac{r_{\mu-k} + r_{\mu-k+\operatorname{ind} q} - r_{\mu-k+\operatorname{ind}(q+1)}}{l}$$

égale à 1 lorsque la valeur de k est à conserver, égale à 0 dans le cas contraire. On aura

$$\sum_k r^{k(l-2n)} = \sum_{k=1}^{k=l-1} \frac{r_{\mu-k} + r_{\mu-k+\operatorname{ind} q} - r_{\mu-k+\operatorname{ind}(q+1)}}{l} r^{k(l-2n)},$$

ou, en multipliant par l et remplaçant $r^{k(l-2n)}$ par $r^{kl(l-2n)}$ qui lui est congru, mod l,

$$l \sum_k r^{k(l-2n)} \equiv \sum_{k=1}^{k=l-1} \left[r_{\mu-k} + r_{\mu-k+\operatorname{ind} q} - r_{\mu-k+\operatorname{ind}(q+1)}\right] r^{kl(l-2n)}, \quad (\operatorname{mod} l^2).$$

Il suffit d'évaluer la seconde somme

$$\sum_{k=1}^{k=l-1} r_{\mu-k+\operatorname{ind} q}\, r^{kl(l-2n)},$$

les deux autres s'en déduiront en effet par le changement de q en 1 et en $q+1$. Posons dans cette somme

$$r_{\mu-k+\operatorname{ind} q} = i,$$

i prendra toutes les valeurs : $1, 2, \ldots, l-1$, comme k; on a d'ailleurs

$$r_{\mu-k+\operatorname{ind} q} = i, \quad (\operatorname{mod} l),$$

d'où on tire

$$r^k \equiv -\frac{q}{i}, \quad (\operatorname{mod} l),$$

et par suite

$$r^{kl(l-2n)} \equiv -\frac{q^{l(l-2n)}}{i^{l(l-2n)}}, \quad (\operatorname{mod} l^2),$$

ou encore

$$r^{kl(l-2n)} \equiv -q^{l(l-2n)} i^{l(2n-1)}, \quad (\operatorname{mod} l^2),$$

car $i^{l(l-1)}$ est congru à 1 pour le même module.

On a dès lors

$$l \sum_k r^{k(l-2n)} \equiv -\left[1 + q^{l(l-2n)} - (q+1)^{l(l-2n)}\right] \sum_{i=1}^{i=l-1} i^{l(2n-1)+1}, \quad (\operatorname{mod} l^2).$$

Mais on a, d'après la formule sommatoire de Bernoulli (voir la note du § 137) :

$$\sum i^{l(2n-1)} \equiv (-1)^{\frac{l(2n-1)+1}{2}} B_{\frac{l(2n-1)+1}{2}} \cdot l, \quad (\text{mod } l^2),$$

d'où en divisant par l, revenant au module l, et tenant compte de ce que l'on a

$$\frac{l(2n-1)+1}{2} = n + (2n-1)\frac{l-1}{2}$$

et que l'on a (¹)

$$\frac{B_{n+s\mu}}{n+s\mu} \equiv (-1)^{s}\frac{B_n}{n}, \quad (\text{mod } l),$$

la congruence

$$\sum_k r^{k(l-2n)} \equiv (-1)^n \left[1 + q^{l-2n} - (q+1)^{l-2n}\right] \frac{B_n}{2n}, \quad (\text{mod } l).$$

Or, q peut toujours être choisi de manière à ce que le crochet ne soit pas divisible par l : on a donc bien, en portant l'expression de $\sum_k r^{k(l-2n)}$ dans les congruences ([illegible]) les conditions

$$B_n \frac{d_u^{l-2n} \log(x + e^u y)}{du^{l-2n}} \equiv 0, \quad (\text{mod } l),$$

qu'il s'agissait de démontrer.

§ III. — *Impossibilité de l'équation* (1) *en nombres entiers x, y, z premiers à l, quand l ne divise qu'un des $\frac{l-3}{2}$ premiers nombres de Bernoulli.*

Théorème III. — Si le nombre premier l ne divise que l'un des $\frac{l-3}{2}$ premiers nombres de Bernoulli et qu'une seule fois, l'équation (1) est impossible en nombres entiers x, y, z premiers à l. [Kummer[16].]

Soit ν le rang du nombre de Bernoulli B_ν qui est divisible par l.

Si ν n'est pas $\frac{l-3}{2}$, on doit avoir, d'après le théorème II, la congruence

$$\frac{d_u^3 \log(x + e^u y)}{du^3} \equiv 0, \quad (\text{mod } l),$$

c'est-à-dire

$$\frac{xy(x-y)}{(x+y)^3} \equiv 0, \quad (\text{mod } l),$$

(¹) Kummer, *Ueber eine allgemeine Eigenschaft der rationalen Entwicklungs-coefficienten einer bestimmten Gattung analytischen Functionen.* (J. de Crelle, t. XLI.) On pourra se contenter de voir P. Bachmann : *Niedere Zahlentheorie. Zweiter Teil. Erstes Kapitel.*

ainsi que les congruences analogues, relatives aux autres combinaisons de x, y, z. On doit donc avoir $x \equiv y$ et, par suite, $x \equiv y \equiv z$; mais comme on doit avoir, d'après le théorème de Fermat,

$$x + y + z \equiv 0, \quad (\text{mod } l),$$

il en résulterait $3x \equiv 0$, ce qui est impossible, l n'étant pas égal à 3.

ν ne pourrait donc être égal qu'à $\frac{l-3}{2}$; mais alors on aurait, d'après le critérium,

$$\frac{d_0^5 \log (x + e^u y)}{du^5} \equiv 0, \quad (\text{mod } l),$$

c'est-à-dire

$$\frac{xy(x-y)(x^2 - 10xy + y^2)}{(x+y)^5} \equiv 0, \quad (\text{mod } l),$$

ou

$$(x-y)(x^2 - 10xy + y^2) \equiv 0, \quad (\text{mod } l),$$

et par suite aussi

$$(x-z)(x^2 - 10xz + z^2) \equiv 0, \quad (\text{mod } l).$$

On ne peut avoir $x \equiv y$, car alors on aurait $z \equiv -2x$ et la deuxième congruence deviendrait

$$3 \,.\, 25 \,.\, x^3 \equiv 0, \quad (\text{mod } l),$$

qui est impossible, l n'étant ni 3 ni 5.

Enfin, on ne peut avoir non plus

$$x^2 - 10xy + y^2 \equiv x^2 - 10xz + z^2 \equiv 0, \quad (\text{mod } l),$$

car, avec $x + y + z \equiv 0$, on en déduirait

$$11\, x(x + 2y) \equiv 0, \quad (\text{mod } l),$$

ce qui est impossible, car on ne peut avoir $x \equiv -2y$, l n'étant ni 3 ni 5, et d'autre part l n'est pas non plus égal à 11, qui est régulier comme 3 et 5. C. q. f. d.

§ IV. — *Recherches récentes sur l'équation* (1) *dans le cas où xyz n'est pas divisible par l.*

Les recherches récentes relatives à l'équation (1), dans le cas où xyz n'est pas divisible par l, ont presque toutes leur origine soit dans les travaux de Kummer, soit dans ceux, plus anciens, de Sophie Germain et de Legendre.

Mirimanoff s'est placé au premier point de vue dans son Mémoire : *L'équation indéterminée $x^l + y^l + z^l = 0$ et le critérium de Kummer*. (J. f. d. r. u. a. Mathematik, tome CXXVIII). En discutant les congruences (5) il a établi le théorème suivant :

THÉORÈME IV. — L'équation (1) est impossible en nombres entiers premiers à l, si les nombres de Bernoulli $B_{\frac{l-3}{2}}$, $B_{\frac{l-5}{2}}$, $B_{\frac{l-7}{2}}$, $B_{\frac{l-9}{2}}$ ne sont pas tous divisibles par l.

D'autre part, il montre qu'on peut éliminer de la façon suivante les nombres de Bernoulli des congruences de Kummer : en désignant par $\varphi_i(t)$, pour $i = 2, 3, \ldots, l-1$, le polynôme

$$\varphi_i(t) = t - 2^{i-1}t^2 + 3^{i-1}t^3 - \ldots + (-1)^{l-2}(l-1)^{i-1}t^{l-1}$$

et par $\varphi_l(t)$ le quotient

$$\varphi_l(t) = \frac{t(1-t^{l-1})}{1+t}.$$

t représentant l'un quelconque des rapports des trois nombres x, y, z, ces congruences équivalent au système

$$\varphi_i\varphi_{l-i+1} \equiv 0, \qquad \left(\bmod l;\ i = 2, 3, \ldots, \tfrac{l-1}{2}\right)$$
$$\varphi_{l-1} \equiv 0.$$

Wieferich (*Zum letzten Fermatschen Theorem*. J. f. d. Mathematik, tome CXXXVI) a déduit des congruences de Mirimanoff le critérium suivant :

THÉORÈME V. — Pour que l'équation (1) puisse avoir une solution, x, y, z étant premiers à l, il faut que le quotient de Fermat

$$q(2) = \frac{2^{l-1}-1}{l}$$

soit divisible par l.

De nouvelles démonstrations, plus simples, de ce critérium ont été données par Frobenius (*Sitzungsberichte der K. Ak. d. Wiss. zu Berlin*, 2 décembre 1909, et *J. f. d. Mathematik*, tome CXXXVII), et par Mirimanoff (*Sur le dernier théorème de Fermat*. J. f. d. Mathematik, tome CXXXIX).

Mirimanoff a montré en outre que :

THÉORÈME VI. — Pour que l'équation (1) puisse avoir une solution, x, y, z étant premiers à l, il faut que le quotient de Fermat

$$q(3) = \frac{3^{l-1}-1}{l}$$

soit divisible par l. (*C. R.*, 24 janvier 1910.)

Dans l'ordre d'idées de Legendre, Dickson part du théorème de Sophie Germain que nous reproduisons :

THÉORÈME VII. — S'il existe un nombre premier impair p tel que la congruence

$$x^n + y^n + z^n \equiv 0, \qquad (\bmod p),$$

soit impossible en nombres entiers premiers à p et tel de plus que n ne soit pas

résidu de puissance $n^{\text{ième}}$, module p, l'équation $x^n + y^n + z^n = 0$ n'a pas de solution en nombres entiers x, y, z premiers à n.

Il en déduit par des méthodes nouvelles l'impossibilité de l'équation (1) avec $xyz \not\equiv 0$, mod. l, pour tout nombre premier l inférieur à 6857. (Dickson, *On the last theorem of Fermat*, février 1908. *Messenger of Mathematics*, tome XXXVIII, et deuxième note, mai 1908, *Quarterly Journal of. P. a A. Mathematics*, tome XL.)

II. — Étude du cas où xyz est divisible par l.

§ V.

Nous allons, avec Kummer, examiner le cas particulier où l remplit les trois conditions suivantes :

1° l divise un seul B_ν des $l - 3$ premiers nombres de Bernoulli et une seule fois;

2° il existe un module pour lequel l'unité

$$E_\nu = \varepsilon(s\varepsilon)^{r^{-2\nu}} \dots (s^{\lambda-1}\varepsilon)^{r^{-2\nu(\lambda-1)}},$$

où ε désigne l'unité circulaire définie au paragraphe 138 :

$$\varepsilon = \sqrt{\frac{(1-\zeta^{r})(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}},$$

n'est pas résidu de $l^{\text{ième}}$ puissance;

3° $B_{\nu l}$ n'est pas divisible par l^3.

Dans ces conditions, l'équation (1) est impossible, même avec l'un des nombres x, y, z divisible par l. [Kummer[16].]

Pour arriver à la démonstration, un certain nombre de théorèmes préliminaires sont nécessaires : ils feront l'objet des paragraphes VI, VII, VIII, IX et X. Auparavant, démontrons d'abord le

Théorème VIII. — Les deux premières hypothèses faites entraînent que le second facteur du nombre des classes n'est pas divisible par l.

Pour cela, nous allons montrer que, dans la première hypothèse, *ce second facteur* $\frac{\Delta}{R}$ *ne peut être divisible par* l *que si l'unité* E_ν *est la* $l^{\text{ième}}$ *puissance d'une unité.*

Reprenons en effet les notations du paragraphe 139 : si $\frac{\Delta}{R}$ est divisible par l, le déterminant du système (117) :

$$\log \varepsilon_i = \sum_{k=1}^{\lambda-1} M_{i,k} \log \eta_k, \qquad (i = 1, 2, \dots, \lambda - 1),$$

l'est aussi ; d'où l'existence de $\mu - 1$ nombres N_i, non tous divisibles par l, et tels que toutes les sommes $\sum_i N_i M_{ii}$ le soient : l'unité $\prod_i \varepsilon_i^{N_i}$ est donc la $l^{\text{ième}}$ puissance d'une unité E et on en déduit, comme au paragraphe 139 :

$$B_i N_i \equiv 0, \quad (\text{mod } l), \qquad (i = 1, 2, \ldots, \mu - 1).$$

Or, les B_i sont tous $\not\equiv 0$, (mod l), excepté B_ν ; il faut donc que tous les N_i soient $\equiv 0$, excepté N_ν. On a, par suite, E′ désignant une unité :

$$E^l = E'^l \varepsilon_\nu^{N_\nu}.$$

Exprimons ε_ν avec les unités circulaires selon la formule (109)

$$\varepsilon_\nu = \varepsilon^{(l-1)F(s)} = \varepsilon^{n_0}(s\varepsilon)^{n_1} \ldots (s^{\mu-2}\varepsilon)^{n_{\mu-2}},$$

où l'exposant symbolique F(s) est égal à $\dfrac{1 - s^\mu}{(1 - s)(r^{2\nu} - s)}$, de sorte qu'on a les congruences

$$n_i \equiv \frac{1 - r^{-2(i+1)\nu}}{1 - r^{2\nu}}, \quad (\text{mod } l), \qquad (i = 0, 1, \ldots, \mu - 2).$$

Posant alors

$$N_\nu \equiv - m r^{2\nu}(1 - r^{2\nu}), \quad (\text{mod } l),$$

on aura pour l'exposant de $s^i\varepsilon$ dans E^l :

$$N_\nu n_i \equiv m r^{2\nu}(r^{-2(i+1)\nu} - 1), \quad (\text{mod } l), \qquad (i = 0, 1, \ldots, \mu - 2).$$

On introduit aisément l'unité $s^{\mu-1}\varepsilon$ en tenant compte de ce que la norme est 1, et on arrive à la formule

$$E''^l = E_\nu^m,$$

E″ désignant une unité et E_ν étant $\varepsilon(s\varepsilon)^{r^{-2\nu}} \ldots (s^{\mu-1}\varepsilon)^{r^{-2(\mu-1)\nu}}$.

Enfin, m n'étant pas divisible par l, on peut déterminer deux entiers a et b, tels que $am = 1 + bl$, de sorte qu'en élevant $E''^l = E_\nu^m$ à la puissance $a^{\text{ième}}$ et remplaçant am par $1 + bl$, on a

$$E_\nu = E'''^l,$$

E‴ désignant une unité.

Dans ce cas, l'unité E_ν est donc résidu de $l^{\text{ième}}$ puissance pour tous les modules.

Si donc nous supposons qu'il existe un module pour lequel l'unité E_ν n'est pas résidu de $l^{\text{ième}}$ puissance, le second facteur du nombre de classes n'est pas divisible par l. C. q. f. d.

§ VI. — *Définition et propriétés des logarithmes pour le module l^{n+1}.*

Soit $f(\zeta)$ un nombre non divisible par $\mathfrak{l}$, c'est-à-dire tel que $f(1)$ ne soit pas divisible par l. Posons, pour abréger,

$$x = 1 - \frac{f(\zeta)}{f(1)},$$

et considérons le développement purement formel

$$x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \ldots + \frac{(-1)^{i-1}}{i}x^i + \ldots,$$

qui serait égal à $\log(1-x)$, si l'on avait $|x| < 1$.

Nous allons montrer que le nombre des termes de ce développement non divisibles par l^{n+1} est limité, et nous *conviendrons* de dire que cet ensemble de termes est congru pour le module l^{n+1} au logarithme de $\frac{f(\zeta)}{f(1)}$: nous écrirons

$$(7) \qquad \log\left[\frac{f(\zeta)}{f(1)}\right] \equiv x - \frac{1}{2}x^2 + \frac{1}{3}x^3 - \ldots, \quad (\mathrm{mod}\ l^{n+1}),$$

en employant le même signe log que pour les logarithmes népériens, mais uniquement comme notation abrégée. [Kummer[17]].

x est divisible par $1-\zeta$, c'est-à-dire par l'idéal $\mathfrak{l}$, et l est égal à $\mathfrak{l}^{l-1}$; un terme quelconque du développement est divisible par une puissance de $\mathfrak{l}$, — par $\mathfrak{l}^m$, si le rang m de ce terme n'est pas divisible par l, et, si ce rang est ml^a, m n'étant pas divisible par l, par $\frac{\mathfrak{l}^{ml^a}}{\mathfrak{l}^{(l-1)a}}$, où l'exposant du numérateur est toujours supérieur à celui du dénominateur ; l'exposant de cette puissance de $\mathfrak{l}$ augmente indéfiniment dans les deux cas avec m, il finira donc par être supérieur à $(n+1)(l-1)$, ce qui montre qu'à partir d'un certain rang tous les termes sont divisibles par l^{n+1}.

Théorème IX. — On a, au sens qui vient d'être défini, la congruence

$$(8) \qquad (l-1)\log\left[\frac{f(\zeta)}{f(1)}\right] \equiv \log\left[\frac{\mathrm{N}f(\zeta)}{f(1)^{l-1}}\right] + \sum_{h=1}^{h=l-2} \frac{d_0^{hl^n}\log f(e^u)}{du^{hl^n}} \mathrm{X}_h(\zeta), \quad (\mathrm{mod}\ l^{n+1}),$$

$\mathrm{N}f(\zeta)$ désignant la norme, l'indice o indiquant que l'on fait $u = 0$ dans les dérivées $hl^{n\,\text{ièmes}}$ de $\log f(e^u)$, et $\mathrm{X}_h(\zeta)$ désignant le polynôme

$$(9) \qquad \mathrm{X}_h(\zeta) = \zeta + r^{-hl^n}\zeta^r + r^{-2hl^n}\zeta^{r^2} + \ldots + r^{-(l-2)l^n}\zeta^{r^{l-2}},$$

où r est une racine primitive pour le module l. [Kummer[12].]

Ordonnons, en effet, la différence $f(1)-f(\zeta)$ suivant les puissances de $1-\zeta$, de sorte que l'on ait

$$f(1)-f(\zeta)=A_1(1-\zeta)+A_2(1-\zeta)^2+\dots+A_{l-1}(1-\zeta)^{l-1},$$

les A_i étant des entiers rationnels. On en déduit

$$(10) \qquad \log\left[\frac{f(\zeta)}{f(1)}\right] \equiv \sum_i \frac{C_i(1-\zeta)^i}{i\,f(1)^i}, \qquad (\text{mod } l^{n-1}).$$

Remplaçons ζ successivement par tous ses conjugués $\zeta^r, \zeta^{r^2}, \dots, \zeta^{r^h}, \dots, \zeta^{r^{l-2}}$, puis ajoutons toutes ces égalités multipliées respectivement par r^{-hkl^n}; on a

$$\sum_{h=0}^{h=l-2} r^{-hkl^n} \log\left[\frac{f(\zeta^{r^h})}{f(1)}\right] \equiv \sum_{h=0}^{h=l-2} \sum_i \frac{C_i r^{-hkl^n}(1-\zeta^{r^h})^i}{i\,f(1)^i}.$$

On a, en développant $(1-\zeta^{r^h})^i$ et sommant d'abord par rapport à h,

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1-\zeta^{r^h})^i}{i} = \sum_{h=0}^{h=l-2} \sum_{s=0}^{s=i} (-1)^s \frac{i!}{i.s!(i-s)!} r^{-hkl^n}\zeta^{sr^h} = \sum_{s=0}^{s=i} (-1)^s \frac{i!}{i.s!(i-s)!} \Lambda_s(\zeta).$$

En désignant alors par P_t la somme

$$P_t=(-1)^t\left[\frac{i!}{t!(i-t)!}-\frac{i!}{(t+l)!(i-t-l)!}+\frac{i!}{(t+2l)!(i-t-2l)!}-\dots\right]$$

et en partageant la somme $\sum_{s=0}^{s=i}$ en l sommes partielles, correspondant respectivement à $s=0$, $s\equiv 1$, ..., $s\equiv l-1$, (mod l), on obtient

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1-\zeta^r)^i}{i} = \frac{1}{i}\left[P_0\Lambda_k(1)+P_1\Lambda_k(\zeta)+\dots+P_{l-1}\Lambda_k(\zeta^{l-1})\right].$$

Pour transformer cette égalité en congruence relative au module l^{n-1}, démontrons d'abord que P_t contient toujours autant de facteurs l que i. Si t n'est pas nul, chaque terme de P_t contient l autant de fois que i : c'est ce qu'il est aisé de voir, à l'aide du théorème suivant, facile à démontrer :

« Si p est un nombre premier et que le nombre A soit représenté dans le système de numération de base p par

$$A=a+a_1p+\dots+a_{m-1}p^{m-1},$$

l'exposant de la plus haute puissance de p qui divise A ! est

$$\frac{A-(a+a_1+\dots+a_{m-1})}{p-1} \text{ ».}$$

[Kummer[12].]

Quant à P_0, il contient de même autant de facteurs l que i, car la somme $P_1 + P_2 + \ldots + P_{l-1}$ étant la somme des coefficients binômiaux alternativement changés de signe est égale à $(1-1)^i = 0$.

Les $\dfrac{P_t}{i}$ peuvent donc être considérés comme des entiers pour le module l^{n+1}, et l'on a, pour toute valeur de i, en tenant compte des congruences $X_k(\zeta^s) \equiv s^{kl^n} X_k(\zeta)$ et $X_k(1) \equiv 0$, (mod l^{n+1}) :

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1-\zeta r^h)^i}{i} \equiv \frac{1}{i}\left[1^{kl^n} P_1 + 2^{kl^n} P_2 + \ldots + (l-1)^{kl^n} P_{l-1}\right] X_k(\zeta), \quad (\mathrm{mod}\ l^{n+1}).$$

Si l'on développe, d'autre part, $(1-e^u)^i$ par la formule du binôme et que l'on prenne la kl^n ième dérivée pour $u=0$, on a

$$\frac{d_0^{kl^n}(1-e^u)^i}{du^{kl^n}} = \sum_{s=0}^{s=i} (-1)^s \frac{i!}{s!(i-s)!} s^{kl^n};$$

d'où, en décomposant cette somme comme plus haut et tenant compte de la congruence

$$(s+ml)^{kl^n} \equiv s^{kl^n}, \quad (\mathrm{mod}\ l^{n+1}),$$

on déduit la congruence

$$\frac{d_0^{kl^n}(1-e^u)^i}{du^{kl^n}} \equiv \left[1^{kl^n} P_1 + 2^{kl^n} P_2 + \ldots + (l-1)^{kl^n} P_{l-1}\right], \quad (\mathrm{mod}\ l^{n+1}).$$

On a, par suite,

$$\sum_{h=0}^{h=l-2} \frac{r^{-hkl^n}(1-\zeta r^h)^i}{i} \equiv \frac{1}{i} \frac{d_0^{kl^n}(1-e^u)^i}{du^{kl^n}} \cdot X_k(\zeta), \quad (\mathrm{mod}\ l^{n+1}),$$

et

$$\sum_{h=0}^{h=l-2} r^{-hkl^n} \log\left[\frac{f(\zeta r^h)}{f(1)}\right] \equiv \sum_i \frac{C_i}{i f(1)^i} \cdot \frac{d_0^{kl^n}(1-e^u)^i}{du^{kl^n}} \cdot X_k(\zeta), \quad (\mathrm{mod}\ l^{n+1}).$$

Or, d'après (10), la somme $\sum_i \dfrac{C_i(1-e^u)^i}{i f(1)^i}$ n'est autre chose que le développement, ordonné suivant les puissances de $1-e^u$, de $\log\left[\dfrac{f(e^u)}{f(1)}\right]$, c'est-à-dire de $\log f(e^u) - \log f(1)$ (¹).

(¹) log désigne ici le logarithme népérien, car e^u étant égal à 1 pour $u=0$, le développement par la série de Mac Laurin est convergent dans le voisinage de $u=0$.

On a donc

$$(11)\qquad \sum_{h=0}^{h=l-2} r^{-hkl^n} \log\left[\frac{f(\zeta^{r^h})}{f(1)}\right] \equiv \frac{d_0^{kl^n}\log f(e^u)}{du^{kl^n}} \cdot X_k(\zeta), \qquad (\text{mod } l^{n+1}).$$

Donnant alors à k les valeurs $1, 2, \ldots, l-2$, faisant la somme, et mettant à part la valeur $h=0$, on obtient, en remarquant que $r^{-hl^n} + r^{-2hl^n} + \ldots + r^{-(l-2)hl^n}$ est congru à -1 pour le module l^{n+1},

$$(l-1)\log\left[\frac{f(\zeta)}{f(1)}\right] \equiv \log\left[\frac{Nf(\zeta)}{f(1)^{l-1}}\right] + \frac{d_0^{l^n}\log f(e^u)}{du^{l^n}} X_1(\zeta) + \ldots, \qquad (\text{mod } l^{n+1}),$$

c'est-à-dire la formule (8) qu'il s'agissait de démontrer.

Cas particulier. — Dans le cas particulier de $n=0$, on a simplement, comme $Nf(\zeta)$ est congru à 1, ainsi que $f(1)^{l-1}$, pour le module l :

$$(12)\qquad -\log\left[\frac{f(\zeta)}{f(1)}\right] \equiv \frac{d_0\log f(e^u)}{du} X_1(\zeta) + \frac{d_0^2\log f(e^u)}{du^2} X_2(\zeta) + \ldots$$
$$+ \frac{d_0^{l-2}\log f(e^u)}{du^{l-2}} X_{l-2}(\zeta), \qquad (\text{mod } l),$$

car on a $\log\left[\frac{Nf(\zeta)}{f(1)^{l-1}}\right] \equiv 0$, (mod l), vu le théorème X qui va être démontré.

Application. — Comme application, nous calculerons le logarithme, pour le module l, de l'unité fréquemment employée

$$E_n(\zeta) = \varepsilon(\zeta) \cdot \varepsilon(\zeta^r)^{r^{-2n}} \cdot \varepsilon(\zeta^{r^2})^{r^{-4n}} \ldots \varepsilon(\zeta^{r^{\mu-1}})^{r^{-2(\mu-1)n}},$$

expression où $\varepsilon(\zeta)$ désigne l'*unité circulaire* (§§ 98 et 138)

$$\varepsilon(\zeta) = \sqrt{\frac{\zeta^{r}-1}{\zeta-1} \cdot \frac{\zeta^{-r}-1}{\zeta^{-1}-1}}.$$

On a

$$\log\left[\frac{E_n(\zeta)}{E_n(1)}\right] = \sum_{h=0}^{h=\mu-1} r^{-2hn}\log\left[\frac{\varepsilon(\zeta^{r^h})}{\varepsilon(1)}\right] \equiv \frac{1}{2}\sum_{h=0}^{h=2\mu-1} r^{-2hn}\log\left[\frac{\varepsilon(\zeta^{r^h})}{\varepsilon(1)}\right], \qquad (\text{mod } l),$$

la congruence des deux derniers membres résulte des relations

$$r^{h+\mu} \equiv -r^h, \qquad \text{et} \qquad r^{-2(h+\mu)n} \equiv r^{-2hn}, \qquad (\text{mod } l),$$

et de ce que $\varepsilon(\zeta^{r^{h+\mu}}) = \varepsilon(\zeta^{-r^h}) = \varepsilon(\zeta^{r^h})$.

On a donc, d'après la formule (9), où l'on prend $n=0$ et $f(\zeta)=\varepsilon(\zeta)$, la congruence

$$\log\left[\frac{E_n(\zeta)}{E_n(1)}\right] \equiv \frac{1}{2}\frac{d_0^{2n}\log\varepsilon(e^u)}{du^{2n}} X_{2n}(\zeta), \qquad (\text{mod } l).$$

Pour calculer la dérivée qui figure dans le second membre, partons du développement connu

$$\frac{1}{e^u-1}=\frac{1}{u}-\frac{1}{2}+\frac{B_1 u}{2!}-\frac{B_2 u^3}{4!}+\frac{B_3 u^5}{6!}-\dots$$

qui donne, si l'on change u en ru et qu'on retranche le développement ci-dessus du nouveau multiplié par r :

$$\frac{r}{e^{ru}-1}-\frac{1}{e^u-1}=-\frac{1}{2}(r-1)+\frac{(r^2-1)B_1 u}{2!}-\frac{(r^4-1)B_2 u^3}{4!}+\dots,$$

et en intégrant :

$$\log\left[\frac{e^{ru}-1}{e^u-1}\right]-(r-1)u=\log r-\frac{1}{2}(r-1)u+\frac{(r^2-1)B_1 u^2}{2\,.\,2!}-\dots,$$

la constante d'intégration étant égale à $\log r$, comme on le voit en faisant $u=0$; on a, par suite,

$$\log \varepsilon(e^u)=\log\left(\frac{e^{ru}-1}{e^u-1}\cdot\frac{e^{-\frac{1}{2}ru}}{e^{-\frac{1}{2}u}}\right)=\log r+\frac{(r^2-1)B_1 u^2}{2\,.\,2!}-\frac{(r^4-1)B_2 u^4}{4\,.\,4!}+\dots.$$

On a, dès lors,

(13) $$\frac{d_0^{2n}\log\varepsilon(e^u)}{du^{2n}}=(-1)^{n-1}(r^{2n}-1)\frac{B_n}{2n},$$

et enfin

(14) $$\log\left[\frac{E_n(\zeta)}{E_n(1)}\right]\equiv(-1)^{n-1}(r^{2n}-1)\frac{B_n}{4n}X_{2n}(\zeta), \qquad (\text{mod } l).$$

Remarque. — L'utilité des logarithmes pour le module l^{n+1} tient, d'une part, à ce que, évidemment, ces développements ont la propriété fondamentale qui correspond à celle des logarithmes eux-mêmes : le logarithme d'un produit est congru à la somme des logarithmes des facteurs ; — et, d'autre part, au théorème suivant :

Théorème X. — Deux nombres congrus pour le module l^{n+1}, ainsi que les entiers qu'on en déduit par la substitution de 1 à ζ, ont aussi leurs logarithmes congrus pour le même module. [Kummer [12].]

Démonstration. — Si, en effet, $f(\zeta)$ et $\varphi(\zeta)$ sont ces deux nombres et qu'on pose

$$x=\frac{f(\zeta)-f(1)}{f(1)}, \qquad y=\frac{\varphi(\zeta)-\varphi(1)}{\varphi(1)},$$

on aura

$$\left.\begin{aligned}\log\left[\frac{f(\zeta)}{f(1)}\right]&\equiv x-\frac{1}{2}x^2+\frac{1}{3}x^3-\dots\\ \log\left[\frac{\varphi(\zeta)}{\varphi(1)}\right]&\equiv y-\frac{1}{2}y^2+\frac{1}{3}y^3-\dots\end{aligned}\right\}(\text{mod } l^{n+1}).$$

On a, vu les hypothèses,

$$x \equiv y, \quad (\mathrm{mod}\ l^{n+1}),$$

d'où évidemment

$$\frac{x^k}{k} \equiv \frac{y^k}{k}, \quad (\mathrm{mod}\ l^{n+1}),$$

au moins si k n'est pas divisible par l. Mais cette congruence est vraie même si k est un multiple de l, soit cl^a, l^a étant la plus haute puissance de l qui entre dans k : car en posant

$$y = x + l^{n+1}z,$$

la formule du binôme donne

$$y^{cl^a} \equiv x^{cl^a} + cl^{n+a+1}x^{cl^a-1}z \quad (\mathrm{mod}\ l^{n+a+2}),$$

et, par suite,

$$\frac{y^{cl^a}}{cl^a} \equiv \frac{x^{cl^a}}{cl^a}, \quad (\mathrm{mod}\ l^{n+1}).$$

Les deux développements $\log\left[\frac{f(\zeta)}{f(1)}\right]$ et $\log\left[\frac{\varphi(\zeta)}{\varphi(1)}\right]$ étant congrus terme à terme, le théorème est démontré.

§ VII. — *Expression de l'indice de l'unité* $E_n(\zeta)$.

Étant donné un idéal premier quelconque $\mathfrak{p}$, de degré f, il est possible de déterminer une racine primitive ρ (¹) de cet idéal, telle que l'on ait

$$\zeta = \rho^{\frac{p^f-1}{l}},$$

p désignant le nombre premier divisible par $\mathfrak{p}$. Cette racine étant ainsi déterminée, l'indice d'un nombre quelconque α du corps $c(\zeta)$ est le même, soit qu'on le prenne par rapport à la racine ρ, soit qu'on le définisse comme au paragraphe 113. En d'autres termes, si l'on pose

$$\alpha \equiv \rho^{I}, \quad (\mathfrak{p}), \qquad \left(\frac{\alpha}{\mathfrak{p}}\right) = \zeta^{I'} \equiv \alpha^{\frac{p^f-1}{l}}, \quad (\mathfrak{p}),$$

on a toujours

$$I \equiv I', \quad (l).$$

Pour déterminer l'indice de l'unité $E_n(\zeta)$, nous allons d'abord établir les propriétés fondamentales du nombre

$$\Psi_q(\zeta) = \sum \zeta^{-(q+1)h+\mathrm{Ind}.(\rho^h+1)}$$

(¹) Voir Hilbert, paragraphe 9.

où l'indice a la signification qu'on vient de rappeler et où la sommation s'étend à toutes les valeurs

$$h = 0, 1, 2, \ldots, p^f - 2,$$

à l'exception de

$$h = \frac{1}{2}(p^f - 1),$$

valeur pour laquelle $\rho^h + 1$ serait congru à zéro, et pour laquelle l'indice n'aurait pas de sens. [Kummer [12].]

Première propriété fondamentale : Ψ_q ne dépend que des périodes à f termes. En effet, on a

$$(\rho^h + 1)^p \equiv \rho^{hp} + 1, \quad (\text{mod } p) \text{ et par suite } (\text{mod } \mathfrak{p});$$

donc, on a

$$\Psi_q(\zeta^p) = \sum \zeta^{-(q+1)hp + p\,\mathrm{Ind}(\rho^h+1)} = \sum \zeta^{-(q+1)hp + \mathrm{Ind}(\rho^h+1)^p} = \sum \zeta^{-(q+1)hp + \mathrm{Ind}(\rho^{hp}+1)} = \Psi_q(\zeta),$$

car les hp reproduisent les h à l'ordre près, (mod $p^f - 1$). Comme p est congru à r^e, (mod l), r étant une racine primitive (mod l), puisqu'il appartient à l'exposant f, Ψ_q admet la substitution (ζ, ζ^{r^e}) et ses puissances, et ne dépend, par suite, que des périodes à f termes (¹).

Deuxième propriété fondamentale. On a

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f, \quad (q \not\equiv 0 \text{ et } \not\equiv -1, \text{ mod } l).$$

En effet,

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = \sum\sum \zeta^{-(q+1)(h-k)+\mathrm{Ind}(\rho^h+1)-\mathrm{Ind}(\rho^k+1)} = p^f - 2 + \sum\sum \zeta^{-(q+1)(h-k)+\mathrm{Ind}(\rho^h+1)-\mathrm{Ind}(\rho^k+1)},$$

le dernier membre étant obtenu en prenant d'abord $h = k$, ce qui donne $p^f - 2$ termes égaux à 1, et la somme double s'étendant ensuite à toutes les valeurs inégales de h et k.

Posons

$$\rho^{h-k} \equiv \rho^{k'}, \qquad \frac{\rho^k + 1}{\rho^h + 1} \equiv \rho^{h'}, \quad (\mathfrak{p});$$

il vient

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f - 2 + \sum\sum \zeta^{(q+1)k'-h'}, \qquad (h', k' = 1, 2, \ldots, p^f - 2, \ h' \neq k'),$$

ou encore

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f - 2 - \sum \zeta^{qk'} + \sum\sum \zeta^{(q+1)k'-h'}.$$

(¹) $ef = l - 1$.

h' et k' pouvant alors être égaux dans la somme double. En sommant par rapport à h', on trouve $\Sigma\zeta^{-h'} = -1$, donc

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f - 2 - \Sigma\zeta^{qk'} - \Sigma\zeta^{(q+1)k'},$$

et, par suite, si q est $\not\equiv 0$ et $\not\equiv -1$ (mod l), on a

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f.$$

Si $q \equiv 0$ ou $\equiv -1$, mod l, la relation donne $\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = +1$, comme cela résulte de $\Psi_0 = \Psi_{l-1} = -1$, et de $\Psi_{q+l} = \Psi_q$.

Troisième propriété fondamentale. Si f est pair, on a

$$\Psi_q(\zeta) = p^{\frac{f}{2}};$$

si f est impair, on a

$$\Psi_q(\zeta) = \pm\,\mathfrak{p}^{m_0}(s\mathfrak{p})^{m_1}\ldots(s^{e-1}\mathfrak{p})^{m_{e-1}},$$

expression où les exposants m_i ont les valeurs suivantes [1] :

$$m_i = \mathrm{S}_{\mu-i} + \mathrm{S}_{\mu-i+\mathrm{ind}\,q} - \mathrm{S}_{\mu-i+\mathrm{ind}(q+1)},$$

S_h désignant la somme

$$\mathrm{S}_h = \frac{1}{l}(r_h + r_{h+e} + \ldots + r_{h+(f-1)e}).$$

La première partie de l'énoncé résulte immédiatement de ce que l'on a $p^{\frac{f}{2}} \equiv -1$, (mod l), et, par suite, $\Psi_q(\zeta^{-1}) = \Psi_q(\zeta^{p^{\frac{f}{2}}}) = \Psi_q(\zeta)$, et de la relation $\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f$.

En vertu de cette même relation, il est clair aussi, pour f impair, que Ψ_q ne peut contenir que l'idéal premier $\mathfrak{p}$ et ses conjugués, et il ne reste qu'à déterminer leurs exposants et l'unité dont le produit est affecté.

Pour cela, nous allons substituer à ζ une puissance de ρ qui lui soit congrue (mod $\mathfrak{p}^n$). Posons pour abréger

$$l' = \frac{p^f - 1}{l},$$

on a successivement

$$\zeta^p \equiv \rho^{l'p}, \qquad (\mathfrak{p}^2),$$
$$\zeta^{p^k} \equiv \rho^{l'p^k}, \qquad (\mathfrak{p}^{k+1}),$$
$$\zeta^{p^{nf}} = \zeta \equiv \rho^{l'p^{nf}}, \qquad (\mathfrak{p}^{nf+1}).$$

---

[1] Ind désigne l'indice par rapport au module $\mathfrak{p}$ et à la racine primitive ρ, ind l'indice par rapport au module l et à la racine primitive r.

Évaluons maintenant $\Psi_q(\zeta^{r_{-i}})$; en posant $q+1 \equiv r^{\kappa}$, (mod l), prenant $\mathrm{Ind}(\rho^{hp''^f}-1)$ au lieu de $\mathrm{Ind}(\rho^h-1)$, on a

$$\Psi_q(\zeta^{r_{-i}}) = \Sigma \zeta^{-hr_{\kappa-i}+r_{-i}\,\mathrm{Ind}(\rho^h+1)},$$

d'où la congruence

$$\Psi_q(\zeta^{r_{-i}}) \equiv \Sigma \rho^{-l'p''^f hr_{\kappa-i}}(\rho^{hp''^f}+1)^{l'p''^f r_{-i}}, \qquad (\mathfrak{p}''^{f+1}),$$

h prenant cette fois dans la somme toutes les valeurs $0, 1, \ldots, q'-2$, la valeur exclue précédemment $h=\frac{1}{2}(p'-1)$ donnant ici un terme $\equiv 0$.

Si l'on développe par la formule du binôme, et qu'on effectue la sommation par rapport à h, il ne reste que les termes où l'exposant de ρ est un multiple de $p'-1=ll'$; soient sll' ces exposants, on a

$$\Psi_q(\zeta^{r_{-i}}) \equiv \Sigma \frac{(p'-1).(l'p''^f r_{-i})!}{(l'r_{\kappa-i}+sll')!\,(l'p''^f r_{-i}-l'r_{\kappa-i}-sll')!}, \qquad (\mathfrak{p}''^{f+1}),$$

ou, en posant

$$s = r_{\kappa-i}\frac{(p''^f-1)}{l} - z$$

et remplaçant $\zeta^{r_{-i}}$ par ζ :

$$\Psi_q(\zeta) \equiv \Sigma \frac{(p'-1)(l'p''^f r_{-i})!}{(l'p''^f r_{\kappa-i}-ll'z)!\,[(r_{-i}-r_{\kappa-i})l'p''^f+ll'z]!}$$

pour le module $(s'\mathfrak{p})^{nf+1}$.

La somme doit être étendue à toutes les valeurs de z qui ne rendent négatifs aucun des deux facteurs du dénominateur. Comme c'est un entier rationnel, tout revient, pour trouver l'exposant de $s'\mathfrak{p}$ dans $\Psi_q(\zeta)$, à trouver quelle est la plus haute puissance de p qui divise la somme Σ.

En s'appuyant sur le théorème relatif aux factorielles énoncé dans le paragraphe V, on trouve aisément, en supposant $r_{-i}-r_{\kappa-i}>0$, que c'est le terme où $z=0$ qui contient p avec le plus petit exposant, et nous avons à calculer le nombre de facteurs p contenus dans

$$Y = \frac{(l'p''^f r_{-i})!}{(l'p''^f r_{\kappa-i})!\,[(r_{-i}-r_{\kappa-i})l'p''^f]!}.$$

Pour cela, cherchons d'une manière générale le nombre de facteurs p contenus dans $(l'p''^f r_h)!$ Soit

$$l'r_h = a + a_1 p + \ldots + a_{f-1}p^{f-1},$$

les a étant inférieurs à p et non négatifs : le nombre des facteurs p de la factorielle sera, d'après le théorème rappelé ci-dessus :

$$\frac{l'p''^f r_h - (a + a_1 + \ldots + a_{f-1})}{p-1}.$$

Multiplions $l'r_h$ par l et remplaçons ll' par $p^f - 1$, nous avons

$$p^f r_h - r_h = la + la_1 p + \ldots + la_{f-1} p^{f-1},$$

d'où, le second membre devant être divisible par p^f :

$$r_h + la = \alpha p,$$
$$\alpha + la_1 = \alpha_1 p,$$
$$\cdots\cdots\cdots$$
$$\alpha_{f-2} + la_{f-1} = \alpha_{f-1} p,$$

les α étant positifs et inférieurs à l; et comme on a $p \equiv r^{me}$, $(\bmod\ l)$, m premier à f, puisque p appartient à l'exposant f, on a les congruences

$$r^h \equiv \alpha r^{me}, \quad \alpha \equiv \alpha_1 r^{me}, \quad \ldots, \quad \alpha_{f-2} \equiv \alpha_{f-1} r^{me}, \quad (\bmod\ l),$$

d'où

$$\alpha \equiv r^{h-me}, \quad \alpha_1 \equiv r^{h-2me}, \quad \ldots, \quad \alpha_{f-1} \equiv r^h, \qquad (\bmod\ l);$$

et comme tous les α sont restes positifs, mod l, on a

$$\alpha = r_{h-me}, \quad \alpha_1 = r_{h-2me}, \quad \ldots, \quad \alpha_{f-1} = r_h.$$

Puis, en ajoutant membre à membre les égalités $r_h + la = ap$, etc., on a :

$$l(a + a_1 + \ldots + a_{f-1}) = (p-1)(r_{h-me} + r_{h-2me} + \ldots + r_h).$$

D'ailleurs, le dernier facteur du second membre est égal, à l'ordre des termes près, à

$$r_h + r_{h+e} + \ldots + r_{h+(f-1)e},$$

parce que m est premier à f. Désignons par lS_h cette somme, qui est en effet divisible par l (¹); on aura pour le nombre de facteurs p de la factorielle :

$$\frac{l'p^{nf}r_h}{p-1} - S_h.$$

Posant pour abréger $r_{-i} - r_{\kappa-i} = \delta$, entier positif et inférieur à l, on aura pour le nombre de facteurs p de N, c'est-à-dire pour l'exposant m_i :

$$m_i = S_{\kappa-i} + S_\delta - S_{-i}.$$

Et pour obtenir l'expression de l'énoncé, il suffit de remarquer que l'on a

$$S_{h+\mu} = f - S_h$$

et que de l'expression de S résulte la congruence

$$r^{-i} - r^{\kappa-i} \equiv \delta \equiv r^{-i} - (q+1)r^{-i} \equiv -qr^{-i} \equiv r^{\mu} r^{-i} r^{\operatorname{ind} q},$$

d'où l'on déduit $\delta = r_{\mu-i+\operatorname{ind} q}$.

(¹) Excepté pour $f = 1$, cas déjà traité paragraphe 1.

Il reste, pour achever la démonstration, à lever la restriction relative au signe de $r_{-i} - r_{\varkappa-i}$. Or, de $r_{\varkappa+h} = l - r_h$ on déduit

$$r_{-i} - r_{\varkappa-i} = -(r_{-i+\mu} - r_{\varkappa-i-\mu}),$$

de sorte que si i ne vérifie pas la condition $r_{-i} - r_{\varkappa-i} > 0$, $\mu - i$ la vérifie. D'autre part, si l'on fait le produit $\Psi_q(\zeta)\Psi_q(\zeta^{-1})$, qui est égal à p^f, il en résulte $m_i + m_{i+\mu} = f$. On a donc $m_i = f - m_{i+\mu}$, et comme on a aussi $S_h = f - S_{h+\mu}$, on retombe sur la même expression de m_i que dans la première hypothèse.

Enfin l'unité $E(\zeta)$, qui affecte le produit des idéaux premiers, est égale à ± 1, car, d'une part, elle ne doit dépendre que des périodes à f termes ($f > 1$), et, d'autre part, on doit avoir $E(\zeta)E(\zeta^{-1}) = 1$ à cause de l'égalité $\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f$; ceci exige $E(\zeta) = \pm \zeta_k$, et k doit être nul d'après la première condition.

Remarque. — La démonstration précédente s'applique encore aux idéaux du premier degré. Si l'on fait, en effet, $f = 1$,

$$lS_h \text{ se réduit à } r_h, \text{ et } m_i \text{ à } \frac{1}{l}(r_{\mu-i} + r_{\mu-i+\operatorname{ind} q} - r_{\mu-i+\operatorname{ind}(q+1)}),$$

expression prenant la valeur 1 ou la valeur 0, suivant que $s^i\mathfrak{p}$ figure dans $\Psi_q(\zeta)$ avec l'exposant 1 ou l'exposant 0; — c'est le résultat du théorème I.

Cette remarque permet de donner une expression unique pour $\Psi_q(\zeta)$, que f soit égal ou supérieur à 1; on a

$$\Psi_q(\zeta) = \pm \prod_{k=0}^{k=l-2} (s^k\mathfrak{p})^{m_k},$$

l'exposant m_k égal à 0 ou 1 étant donné par la formule

$$m_k = \frac{1}{l}(r_{\mu-k} + r_{\mu-k+\operatorname{ind} q} - r_{\mu-k+\operatorname{ind}(q+1)}).$$

La formule s'applique aussi pour f pair; elle est donc générale.

Indice de $E_n(\zeta)$. — L'identité des propriétés de $\Psi_q(\zeta)$ (1), quel que soit l'exposant auquel appartient le nombre p correspondant, va nous permettre de trouver, par un calcul unique, s'appliquant à tous les cas, une expression de l'indice de $E_n(\zeta)$ à l'aide de ce nombre.

Cette expression est la suivante :

(15) $$\operatorname{Ind} E_n(\zeta) \equiv \frac{r^{2n} - 1}{2} \cdot \frac{1}{1 + q^{l-2n} - (q+1)^{l-2n}} \cdot \frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \pmod{l}.$$

[Kummer[12].]

---

(1) Nous avons utilisé dans le paragraphe 1 et le paragraphe actuel deux formes différentes de $\Psi_q(\zeta)$, mais on passe aisément de l'une à l'autre. (Voir Weber, *Alg. sup.*)

Pour la démontrer, calculons d'abord la dérivée, en partant du développement

$$\Psi_q(e^u) = \sum e^{u[-(q+1)h + \mathrm{Ind}(\rho^h+1)]}.$$

On a, en posant pour abréger,

$$m = l - 2n - 1, \qquad U = \frac{1}{\Psi_q(e^u)},$$

$$\frac{d^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} = \frac{d^m\left(\frac{d\Psi_q(e^u)}{du}\cdot U\right)}{du^m},$$

d'où, par la formule de Leibnitz :

$$\frac{d^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} = \frac{d^{m+1}\Psi_q}{du^{m+1}}\cdot U + \frac{m}{1}\cdot\frac{d^m\Psi_q}{du^m}\cdot\frac{dU}{du} + \ldots$$

Comme

$$\Psi_q(\zeta)\Psi_q(\zeta^{-1}) = p^f,$$

on a

$$\Psi_q(e^u)\Psi_q(e^{-u}) = p^f + VW,$$

où W désigne un polynôme en e^u à coefficients entiers et où

$$V = 1 + e^u + e^{2u} + \ldots + e^{(l-1)u}$$

(parce que la différence $\Psi_q(x)\Psi_q(x^{-1}) - \Psi_q(\zeta)\Psi_q(\zeta^{-1})$, admettant la racine ζ, admet toutes les racines de $1 + x + \ldots + x^{l-1}$).

On a donc

$$\Psi_q(e^{-u}) = U(p^f + VW),$$

$$\frac{d^i\Psi_q(e^{-u})}{du^i} = \frac{d^iU}{du^i}(p^f + VW) + \frac{1}{i}\cdot\frac{d^{i-1}U}{du^{i-1}}\cdot\frac{d(VW)}{du} + \ldots.$$

Pour $u = 0$, V et ses $l-2$ premières dérivées s'annulent, mod l, et comme on a $p^f \equiv 1$, pour ce même module, on déduit du développement précédent

$$\frac{d_0^i\Psi_q(e^{-u})}{du^i} \equiv \frac{d_0^iU}{du^i}, \qquad (\text{mod } l),$$

pour $i = 0, 1, 2, \ldots, l-2$.

On peut encore écrire

$$\frac{d_0^iU}{du^i} \equiv (-1)^i\frac{d_0^i\Psi_q(e^u)}{du^i} \equiv (-1)^i D_i, \qquad (\text{mod } l).$$

Donc, on a

$$\frac{d_0^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv D_{m+1}D_0 - \frac{m}{1}D_mD_1 + \frac{m(m-1)}{1.2}\cdot D_{m-1}D_2 - \ldots, \qquad (\text{mod } l).$$

Mais

$$D_i = \sum[-(q+1)h + \mathrm{Ind}(\rho^h+1)]^i$$

$$\left(h = 0, 1, \ldots, p^f-2, \text{ excepté } \frac{p^f-1}{2}\right).$$

Désignons le crochet par C_h, nous aurons

$$d = \frac{d_u^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \Sigma\Sigma\left(C_h^{m+1} C_k^0 - \frac{m}{1} \cdot C_h^m C_k^1 + \ldots\right), \quad (\text{mod } l),$$

les valeurs $h = \frac{1}{2}(p^f - 1)$, $k = \frac{1}{2}(p^f - 1)$ étant exclues de la sommation, c'est-à-dire

$$d \equiv \Sigma\Sigma C_h (C_h - C_k)^m$$

$$= \Sigma\Sigma[-(q+1)h + \text{Ind}(\rho^h + 1)][-(q+1)(h-k) + \text{Ind}(\rho^h + 1) - \text{Ind}(\rho^k + 1]^m.$$

Comme tous les termes sont congrus à zéro pour $h = k$, employons la transformation déjà utilisée

$$\rho^{k-h} \equiv \rho^{k'}, \quad \frac{\rho^k + 1}{\rho^h + 1} \equiv \rho^{h'}, \quad (\text{mod } \mathfrak{p});$$

nous avons

$$\Sigma\Sigma[-(q+1)\,\text{Ind}(\rho^{h'} - 1) + \text{Ind}(\rho^{k'} - 1) + q\,\text{Ind}(\rho^{k'} - \rho^{h'})][(q+1)k' - h']^m, (\text{mod } l).$$
$$(h', k' = 1, 2, \ldots, p^f - 1,\ h' \neq k)$$

Évaluons séparément les trois sommes correspondant aux termes du premier crochet, en sommant d'abord par rapport à k'; pour plus de facilité, on ajoute dans la somme double les termes où $h' = k'$, en les retranchant d'autre part. La première somme, comme $p^f - 1$ est $\equiv 0$, (mod l), que $\Sigma k'^i$ est $\equiv 0$ pour $i = 1, 2, \ldots, l-2$, et que l'on a

$$\sum_{k'} [(q+1)k' - h']^{l-2n-1} \equiv (p^f - 2)h'^{l-2n-1} \equiv -h'^{l-2n-1},$$

devient

$$(q+1)(1 + q^{l-2n-1})\,\Sigma h'^{l-2n-1}\,\text{Ind}(\rho^{h'} - 1).$$

On trouve de même pour la seconde :

$$-[q^{l-2n-1} + (q+1)^{l-2n-1}]\,\Sigma h'^{l-2n-1}\,\text{Ind}(\rho^{h'} - 1).$$

Pour évaluer la troisième, ajoutons et retranchons les termes relatifs à $h' = 0$ et à $k' = 0$:

$$-q[1 + (q+1)^{l-2n-1}]\,\Sigma h'^{l-2n-1}\,\text{Ind}(\rho^{h'} - 1);$$

le reste de la somme

$$q\Sigma\Sigma[\text{Ind}(\rho^{h'} - 1) + k'](rk' - h')^{l-2n-1} \quad \begin{pmatrix} h' = 1, 2, \ldots, p^f - 2 \\ k' = 0, 1, 2, \ldots, p^f - 2 \end{pmatrix}$$

est congru à zéro.

On a donc en réunissant les trois sommes

$$\frac{d_u^{l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv [1 + q^{l-n} - (q+1)^{l-2n}]\,\Sigma h'^{l-2n-1}\,\text{Ind}(\rho^{h'} - 1), \quad (\text{mod } l).$$

Dans la somme, tous les termes pour lesquels h' est $\equiv 0$, mod l, disparaissent, et si l'on pose $h' = i + lk$ $\left(\begin{smallmatrix} i=1,2,\ldots,l-1 \\ k=0,1,2,\ldots,l'-1 \end{smallmatrix}\right)$, on a

$$\Sigma \equiv \Sigma\Sigma\, i^{l-2n-1} \operatorname{ind}(\rho^{i+kl} - 1).$$

Mais on a évidemment toujours la congruence

$$(\rho^{i} - 1)(\rho^{i+l} - 1)(\rho^{i+2l} - 1)\ldots(\rho^{i+(l'-1)l} - 1) \equiv 1 - \rho^{l'i}, \qquad (\text{mod } \mathfrak{p}),$$

et, par suite,

$$\Sigma \operatorname{Ind}(\rho^{i+kl} - 1) \equiv \operatorname{Ind}(1 - \rho^{l'i}) = \operatorname{Ind}(1 - \zeta^{i}), \qquad (\text{mod } l).$$

Donc, on a

$$\Sigma \equiv \Sigma\, i^{l-2n-1} \operatorname{Ind}(1 - \zeta^{i}), \qquad (\text{mod } l).$$

En remplaçant i par ir, ce qui ne change pas Σ, multipliant par r^{2n} et retranchant l'égalité primitive de la nouvelle, on obtient

$$(r^{2n} - 1)\,\Sigma \equiv \Sigma\, i^{l-2n-1} \operatorname{Ind}\left(\frac{1 - \zeta^{ri}}{1 - \zeta^{i}}\right).$$

Si l'on change enfin i en r^h, on a

$$(r^{2n} - 1)\,\Sigma \equiv \Sigma\, r^{-2nh} \operatorname{Ind}\left(\frac{1 - \zeta^{r^{h+1}}}{1 - \zeta^{r^h}}\right) = 2 \operatorname{Ind} \mathrm{E}_n(\zeta),$$

puisque

$$\mathrm{E}_n(\zeta) = \varepsilon(\zeta)\,\varepsilon(\zeta^{r})^{r^{-2n}} \ldots \varepsilon(\zeta^{r^{\lambda-1}})^{r^{-2(\lambda-1)n}}$$

et que l'on a

$$\varepsilon(\zeta^{r^h}) = \frac{1 - \zeta^{r^{h+1}}}{1 - \zeta^{r^h}} \cdot \zeta^{\frac{r^h(1-r)}{2}}.$$

Par conséquent, on a pour expression de l'indice de $\mathrm{E}_n(\zeta)$, (mod $\mathfrak{p}$) :

$$\operatorname{Ind} \mathrm{E}_n(\zeta) \equiv \frac{r^{2n} - 1}{2} \cdot \frac{1}{1 + q^{l-2n} - (q+1)^{l-2n}} \cdot \frac{d_0^{\,l-2n} \log \Psi_r(e^u)}{du^{l-2n}}, \quad (\text{mod } l). \quad \text{C. q. f. d.}$$

Remarque. — L'indice est $\equiv 0$ pour toute unité E_n, telle que $l - 2n$ ne soit pas divisible par f.

En effet, d'après la première propriété fondamentale de Ψ_q, on a

$$\Psi_q(\zeta) = \Psi_q(\zeta^{r^e}),$$

et, par suite,

$$\Psi_q(e^u) = \Psi_q(e^{ur^e}) + \text{V.W.}$$

et

$$\frac{d_0^{\,l-2n} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \frac{d_0^{\,l-2n} \log \Psi_q(e^{ur^e})}{du^{l-2n}} \equiv r^{(l-2n)e}\, \frac{d_0^{\,l-2n} \log \Psi_q(e^u)}{du^{l-2n}}, \qquad (\text{mod } l).$$

Si donc l'on n'a pas

$$r^{(l-2n)e} - 1 \equiv 0, \qquad (\text{mod } l),$$

c'est-à-dire si $l - 2n$ n'est pas divisible par f, il faut que $\dfrac{d_0^{\,l-2n} \log \Psi_q(e^u)}{du^{l-2n}}$ soit $= 0$, c'est-à-dire que $\operatorname{Ind} \mathrm{E}_n(\zeta) = 0$.

§ VIII. — *Étude des idéaux dont la $l^{\text{ième}}$ puissance est un idéal principal.*

Le résultat final de cette étude est le

Théorème XI. — Moyennant les hypothèses du paragraphe V, la condition nécessaire et suffisante pour qu'un idéal $\mathfrak{i}$, dont la $l^{\text{ième}}$ puissance est idéal principal, soit lui-même principal, est que l'on ait

$$(16)\qquad \frac{d_0^{l-2\nu}\log \mathfrak{i}^l(e^u)}{du^{l-2\nu}} \equiv 0, \qquad (\mathrm{mod}\ l);$$

[Kummer [16].]

La démonstration nécessite quelques développements, qui font l'objet des deux lemmes suivants :

Lemme III. — Si le nombre de classes h est divisible une seule fois par l et qu'un idéal $\mathfrak{i}$ appartienne à l'exposant l, c'est-à-dire si $\mathfrak{i}^l$ est la première puissance de $\mathfrak{i}$ qui soit un idéal principal, les idéaux $1, \mathfrak{i}, \mathfrak{i}^2, \ldots, \mathfrak{i}^{l-1}$ représentent *toutes* les classes d'idéaux appartenant à l'exposant l.

Ces l classes sont évidemment distinctes, puisque $\mathfrak{i}$ appartient à l'exposant l; s'il existait un autre idéal $\mathfrak{i}'$ appartenant à l'exposant l et non équivalent à l'un des précédents, les produits $\mathfrak{i}^m\mathfrak{i}'^{m'}$ représenteraient pour m et m' égaux à $0, 1, 2, \ldots, l-1$, l^2 classes d'idéaux non équivalentes; ensuite $\mathfrak{i}''$ désignant un idéal non équivalent à l'un des idéaux représentés par $\mathfrak{i}^m\mathfrak{i}'^{m'}$, les idéaux $\mathfrak{i}^m\mathfrak{i}'^{m'}\mathfrak{i}''^{m''}$ seraient tous non équivalents pour m et m' égaux à $0, 1, \ldots, l-1$, et m'' égal à $0, 1, \ldots, h''-1$, en désignant par $\mathfrak{i}''^{h''}$ la première puissance de $\mathfrak{i}''$ qui soit équivalente à $\mathfrak{i}^m\mathfrak{i}'^{m'}$. En continuant ainsi on arrive à épuiser le nombre h de toutes les classes, et l'on aurait $h = l^2h''h''' \ldots$, ce qui est impossible si h n'est divisible par l qu'une fois.

Lemme IV. — Si les deux premières hypothèses du paragraphe V sont vérifiées, l'indice de l'unité E_ν, par rapport à un module premier $\mathfrak{p}$, est

$$(17)\qquad \mathrm{Ind}\ E_\nu \equiv \frac{(-1)^{\nu-1}(r^{2\nu}-1)B_\nu l-\nu}{2h} \cdot \frac{d_0^{l-2\nu}\log \mathfrak{p}^h(e^u)}{du^{l-2\nu}}, \qquad (\mathrm{mod}\ l).$$

[Kummer [16].]

En effet, on a démontré la formule générale (15)

$$\mathrm{Ind}\ E_n = \frac{r^{2n}-1}{2} \cdot \frac{1}{1+q^{l-2n}-(q+1)^{l-2n}} \cdot \frac{d_0^{l-2n}\log \Psi_q(e^u)}{du^{l-2n}}, \qquad (\mathrm{mod}\ l).$$

où l'on a

$$\Psi_q(\zeta) = \pm \prod_{k=0}^{k=l-2} (s^k \mathfrak{p})^{m_k}.$$

les exposants m_k étant donnés par la formule

$$m_k = \frac{1}{l}(r_{\mu-k} + r_{\mu-k+\mathrm{ind}\,q} - r_{\mu-k+\mathrm{ind}(q+1)}).$$

En élevant à la puissance $h_1 l = h$, de manière à n'avoir que des idéaux principaux, on a

$$\Psi_q(\zeta)^{h_1 l} = \pm \prod_{k=0}^{k=l-2} (s^k \mathfrak{p})^{h}]^{m_k}.$$

On en déduit

$$h_1 l \frac{d_0^{(l-2n)l} \log \Psi_q(e^u)}{du^{l-2n}} \equiv \sum_{k=0}^{k=l-2} m_k \frac{d_0^{(l-2n)l} \log s^k \mathfrak{p}^h(e^u)}{du^{l-2n}}, \quad (\mathrm{mod}\ l^2),$$

car si deux nombres α et β sont égaux, ou même simplement congrus, mod l^{t+1}, on a pour toute valeur de t non divisible par $l-1$

$$\frac{d_0^{tl^t} \alpha(e^u)}{du^{tl^t}} \equiv \frac{d_0^{tl^t} \beta(e^u)}{du^{tl^t}}, \quad (\mathrm{mod}\ l^{t+1}).$$

On a donc, vu l'expression donnée plus haut de Ind E_n,

$$h_1 l \,\mathrm{Ind}\, E_n \equiv \frac{r^{2n}-1}{2[1+q^{l-2n}-(q+1)^{l-2n}]} \cdot \frac{d_0^{(l-2n)l} \log \mathfrak{p}^h(e^u)}{du^{(l-2n)l}} \cdot \sum_{k=0}^{k=l-2} m_k r^{(l-2n)k}, \quad (\mathrm{mod}\ l^2),$$

en remarquant que $s^k \mathfrak{p}^h(e^u) = \mathfrak{p}^h(e^{ur^k})$, et qu'on peut remplacer la dérivée $(l-2n)^{\text{ième}}$ par la $(l-2n)l^{\text{ième}}$ qui lui est congrue, mod l.

Désignant pour abréger par K la somme Σ_k et remplaçant m_k par sa valeur, on a

$$l\mathrm{K} \equiv \sum_{k=0}^{k=l-2} r^{(l-2n)lk} [r_{\mu-k} + r_{\mu-k+\mathrm{ind}\,q} - r_{\mu-k+\mathrm{ind}(q+1)}], \quad (\mathrm{mod}\ l^2).$$

Remplaçons maintenant $r^{(l-2n)lk}$ par $r^{(l-2n)l^2k}$ qui lui est congru pour le module l^2, nous aurons

$$l\mathrm{K} \equiv \sum_{k=0}^{k=l-2} r_{\mu-k} r^{(l-2n)l^2k} + \sum_{k=0}^{k=l-2} r_{\mu-k+\mathrm{ind}\,q} r^{(l-2n)l^2k} - \sum_{k=0}^{k=l-2} r_{\mu-k+\mathrm{ind}(q+1)} r^{(l-2n)l^2k}, \quad (\mathrm{mod}\ l^2).$$

Il suffit d'évaluer la seconde somme, dont les deux autres se déduisent par le changement de q en 1 ou en $q+1$. Posons

$$r^{\mu k + \mathrm{ind}\, q} = i\,;$$

i prendra toutes les valeurs $1, 2, \ldots, l-1$ quand k prendra les valeurs $0, 1, \ldots, l-2$; puis, de

$$r^{\mu k + \mathrm{ind}\, q} \equiv i, \quad \text{ou} \quad r^{\mu k} \equiv -\frac{q}{i}, \quad (\mathrm{mod}\ l),$$

on tire

$$r^{(l-2n)l^2 k} \equiv -\frac{q^{(l-2n)l^2}}{i^{(l-2n)l^2}}, \quad (\mathrm{mod}\ l^3),$$

ou encore

$$r^{(l-2n)l^2 k} \equiv -q^{(l-2n)l^2}\, i^{(2n-1)l^2}, \quad (\mathrm{mod}\ l^3),$$

parce que l'on a $i^{(l-1)l^2} \equiv 1$, $(\mathrm{mod}\ l^3)$.

La seconde somme est donc congrue à

$$-q^{(l-2n)l^2} \sum_{i=1}^{i=l-1} i^{(2n-1)l^2+1}, \quad (\mathrm{mod}\ l^3),$$

et l'on a

$$l\mathrm{K} \equiv -\left[1 + q^{(l-2n)l^2} - (q+1)^{(l-2n)l^2}\right] \sum_{i=1}^{i=l-1} i^{(2n-1)l^2+1}, \quad (\mathrm{mod}\ l^3).$$

Or, on a

$$\sum_{i=1}^{i=l-1} i^{(2n-1)l^2+1} \equiv (-1)^{n+1} \mathrm{B}_{\frac{(2n-1)l^2+1}{2}} \,.\, l, \quad (\mathrm{mod}\ l^3).$$

En posant, pour abréger,

$$\mathrm{Q} = 1 + q^{l-2n} - (q+1)^{l-2n}, \quad \mathrm{Q}' = 1 + q^{(l-2n)l} - (q+1)^{(l-2n)l},$$

et revenant au module l^2, en divisant par l, on a donc, pour l'expression de l'indice :

$$h_1 l \,\mathrm{Ind}\, \mathrm{E}_n(\zeta) \equiv (-1)^n \frac{(r^{2n}-1)\mathrm{Q}'}{\mathrm{Q}} \,.\, \mathrm{B}_{\frac{(2n-1)l^2+1}{2}} \,.\, \frac{d^{(l-2n)l} \log \mathfrak{p}^h(e^u)}{du^{(l-2n)l}}, \quad (\mathrm{mod}\ l^2).$$

En utilisant la congruence

$$\frac{\mathrm{B}_m}{m} \equiv (-1)^{s\mu} \frac{\mathrm{B}_{m+sl\mu}}{m+sl\mu}, \quad (\mathrm{mod}\ l^2),$$

démontrée dans le Mémoire de Kummer, cité en note au § II, on a, si l'on y fait $m = \frac{(2n-1)l+1}{2} = nl - \mu$ et $s = 2n-1$:

$$\mathrm{B}_{\frac{(2n-1)l^2+1}{2}} \equiv \frac{(-1)^{\mu} \mathrm{B}_{nl-\mu}}{2(nl-\mu)}, \quad (\mathrm{mod}\ l^2).$$

Si l'on fait enfin $n = \nu$, $B_{l\nu}$ est divisible par l, car B_ν l'est : on peut alors diviser par l les deux membres de la congruence qui donne l'indice, et comme on a $Q' \equiv Q$, $(\bmod l)$, et aussi

$$\frac{d_0^{l-2\nu l} \log \mathfrak{p}^h(e^u)}{du^{l-2\nu l}} \equiv \frac{d_0^{l-2\nu} \log \mathfrak{p}^h(e^u)}{du^{l-2\nu}}, \quad (\bmod l),$$

on a finalement

$$\operatorname{Ind} E_\nu(\zeta) \equiv \frac{(-1)^{n+\nu}(r^{2\nu}-1)B_{l\nu}}{2h_1 l} \cdot \frac{d_0^{l-2\nu} \log \mathfrak{p}^h(e^u)}{du^{l-2\nu}}, \quad (\bmod l).$$

C. q. f. d.

Définition. — La formule précédente s'applique encore dans le cas d'un module composé, moyennant une généralisation de la notion d'indice, analogue à celle que Jacobi a donnée du symbole de Legendre. D'après la définition du symbole $\left\{\frac{\alpha}{\mathfrak{p}}\right\}$ (voir § 113), on a

$$\zeta^{\operatorname{Ind} \alpha} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}.$$

On définira le symbole $\left\{\frac{\alpha}{\mathfrak{i}}\right\}$, dans le cas d'un idéal $\mathfrak{i}$ composé, par la relation

$$\left\{\frac{\alpha}{\mathfrak{i}}\right\} = \left\{\frac{\alpha}{\mathfrak{p}}\right\}\left\{\frac{\alpha}{\mathfrak{q}}\right\}\left\{\frac{\alpha}{\mathfrak{r}}\right\}\cdots,$$

$\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, etc., étant les idéaux premiers distincts ou non dont le produit est égal à $\mathfrak{i}$: l'indice par rapport à $\mathfrak{i}$ est la somme des indices pour $\mathfrak{p}$, $\mathfrak{q}$, $\mathfrak{r}$, etc. Le logarithme d'un produit de facteurs étant égal à la somme des logarithmes des facteurs, et l'indice ayant la même propriété, on voit que l'on a encore dans le cas d'un module $\mathfrak{i}$ composé :

$$\operatorname{Ind} E_\nu(\zeta) \equiv \frac{(-1)^{n+\nu}(r^{2\nu}-1)B_{l\nu}}{2h_1 l} \cdot \frac{d_0^{l-2\nu} \log \mathfrak{i}^h(e^u)}{du^{l-2\nu}}, \quad (\bmod l).$$

Remarque I. — Il résulte de là que si l'idéal $\mathfrak{i}$ est principal ou s'il appartient à un exposant non divisible par l, l'indice de $E_\nu(\zeta)$, par rapport à ce module, est divisible par l, c'est-à-dire que

$$\left\{\frac{E_\nu(\zeta)}{\mathfrak{i}}\right\} = 1,$$

car l'exposant a, auquel appartient $\mathfrak{i}^a$, étant un diviseur de $h = h_1 l$, et n'étant pas divisible par l, doit diviser h_1 ; soit $h_1 = a h_2$, on aura $\mathfrak{i}^h = (\mathfrak{i}^a)^{h_2 l}$, et, par suite,

$$\log \mathfrak{i}^h(e^u) = h_2 l \log \mathfrak{i}^a(e^u),$$

d'où

$$\frac{d_0^{l-2\nu} \log \mathfrak{i}^h(e^u)}{du^{l-2\nu}} \equiv 0 \quad \text{et} \quad \operatorname{Ind} E_\nu(\zeta) \equiv 0, \quad (\bmod l).$$

Remarque II. — Il résulte de là que $E_\nu(\zeta)$ a même indice par rapport à deux idéaux équivalents $\mathfrak{a}$ et $\mathfrak{b}$.

Car dans ce cas il existe un idéal $\mathfrak{c}$, tel que $\mathfrak{ac}$ et $\mathfrak{bc}$ soient tous deux principaux, et alors

$$\left\{\frac{E_\nu}{\mathfrak{ac}}\right\} = 1 = \left\{\frac{E_\nu}{\mathfrak{bc}}\right\},$$

ou en supprimant le facteur commun $\left\{\frac{E_\nu}{\mathfrak{c}}\right\}$:

$$\left\{\frac{E_\nu}{\mathfrak{a}}\right\} = \left\{\frac{E_\nu}{\mathfrak{b}}\right\}.$$

Passons maintenant à la *démonstration du théorème XI*.

Par hypothèse, il existe un module $\mathfrak{a}$ pour lequel $E_\nu(\zeta)$ n'est pas reste de $l^{\text{ième}}$ puissance et, par conséquent, $i = \operatorname{Ind} E_\nu(\zeta)$ est $\not\equiv 0$, mod l, ou encore

$$\left\{\frac{E_\nu(\zeta)}{\mathfrak{a}}\right\} = \zeta^i.$$

Il résulte alors de la remarque I précédente que $\mathfrak{a}$ appartient à un exposant divisible par l, soit al, et a n'est pas divisible par l, car autrement le nombre des classes serait divisible par l^2. Ensuite $\mathfrak{b} = \mathfrak{a}^a$ appartient à l'exposant l, et l'on a

$$\left\{\frac{E_\nu(\zeta)}{\mathfrak{b}}\right\} = \zeta^{ai}, \qquad \left\{\frac{E_\nu(\zeta)}{\mathfrak{b}^m}\right\} = \zeta^{aim}.$$

Si maintenant $\mathfrak{i}$ est un idéal dont la $l^{\text{ième}}$ puissance est idéal principal, il est (d'après le lemme IV) équivalent à l'un $\mathfrak{b}^m$ des idéaux

$$1,\ \mathfrak{b},\ \mathfrak{b}^2,\ \ldots,\ \mathfrak{b}^{l-1}.$$

On a donc

$$\left\{\frac{E_\nu(\zeta)}{\mathfrak{i}}\right\} = \left\{\frac{E_\nu(\zeta)}{\mathfrak{b}^m}\right\} = \zeta^{aim}$$

ou

$$\operatorname{Ind} E_\nu(\zeta) \equiv aim, \quad (\operatorname{mod} l),$$

l'indice se rapportant au module $\mathfrak{i}$. Comme ai n'est pas divisible par l, l'indice est ou n'est pas divisible par l, en même temps que m, c'est-à-dire à cause de l'équivalence

$$\mathfrak{i} \sim \mathfrak{b}^m,$$

suivant que $\mathfrak{i}$ est ou n'est pas principal.

Mais puisqu'on suppose que $\mathfrak{i}^l$ est principal, l'expression de l'indice de $E_\nu(\zeta)$ devient (après suppression du facteur h_1 dans les deux termes de la fraction)

$$\operatorname{Ind} E_\nu(\zeta) \equiv \frac{(-1)^{\nu/2}(r^{2\nu}-1)B_{\nu/2}}{2\nu} \cdot \frac{d_0^{l-\nu}\log \mathfrak{i}^l(e^u)}{du^{l-\nu}}, \quad (\operatorname{mod} l).$$

et ~~si~~ l'on observe que le premier facteur du second membre est indépendant de $\mathfrak{i}$ et qu'il n'est certainement pas divisible par l, car autrement $E_\nu(\zeta)$ serait reste de puissance $l^{\text{ème}}$ pour le module $\mathfrak{i}$, contrairement à l'hypothèse, on voit que l'indice de E_ν est ou n'est pas divisible par l, en même temps que $\dfrac{d_0^{l-2\nu}\log \mathfrak{i}^l(e^u)}{du^{l-2\nu}}$, ce qui achève la démonstration du théorème.

Corollaire. — Dans le cas d'un idéal $\mathfrak{i}$ du corps $c(\zeta+\zeta^{-1})$, on a $\mathfrak{i}^l(\zeta)=\mathfrak{i}^l(\zeta^{-1})$, et, par suite, toutes les dérivées d'ordre impair du logarithme sont congrues à zéro pour $u=0$, en particulier la $(l-2\nu)^{\text{ième}}$.

Donc, *tout idéal du corps* $c(\zeta+\zeta^{-1})$, *dont la* $l^{\text{ème}}$ *puissance est un idéal principal, est lui-même idéal principal.*

§ IX. *Condition moyennant laquelle un nombre du corps $c(\zeta+\zeta^{-1})$, multiplié par une unité convenable, est congru, mod l, à un entier rationnel.*

Théorème XII. — Si l ne divise qu'un seul B_ν des $\dfrac{l-3}{2}$ premiers nombres de Bernoulli et qu'une seule fois, tout nombre $F(\zeta)$ du corps $c(\zeta+\zeta^{-1})$, qui vérifie la congruence

$$\frac{d_0^{2\nu}\log F(e^u)}{du^{2\nu}}\equiv 0, \quad (\operatorname{mod} l),$$

peut, après multiplication par une unité convenable, devenir congru, mod l, à un entier rationnel. [Kummer[16].]

On a, en effet, dans ce cas, en appliquant la formule (12) :

$$-\log\left[\frac{F(\zeta)}{F(1)}\right]\equiv\frac{d_0^2\log F(e^u)}{du^2}X_2(\zeta)+\ldots+\frac{d_0^{l-3}\log F(e^u)}{du^{l-3}}X_{l-3}(\zeta), \quad (\operatorname{mod} l),$$

les dérivées d'ordres impairs disparaissant à cause de $F(e^u)=F(e^{-u})$.

Employons maintenant les unités $E_n(\zeta)$, pour lesquelles on a, d'après la formule (14) :

$$\log\left[\frac{E_n(\zeta)}{E_n(1)}\right]\equiv(-1)^{n-1}(r^{2n}-1)\frac{B_n}{4n}X_{2n}(\zeta), \quad (\operatorname{mod} l).$$

Déterminons les entiers X_n pour $n=1, 2, \ldots, \mu-1$, à l'exception de $n=\nu$ par les congruences

$$(-1)^{n+1}(r^{2n}-1)\frac{B_n}{4n}.X_n\equiv\frac{d_0^{2n}\log F(e^u)}{du^{2n}}, \quad (\operatorname{mod} l),$$

nous aurons

$$X_n\log\left[\frac{E_n(\zeta)}{E_n(1)}\right]\equiv\frac{d_0^{2n}\log F(e^u)}{du^{2n}}.X_{2n}(\zeta), \quad (\operatorname{mod} l).$$

et, pour $n = \nu$, on a, quel que soit N_ν, puisque B_ν est supposé divisible par l :

$$N_\nu \log\left[\frac{E_\nu(\zeta)}{E_\nu(1)}\right] \equiv 0, \qquad (\text{mod } l).$$

Par suite, si l'on suppose

$$\frac{d_0^{2\nu} \log F(e^u)}{du^{2\nu}} \equiv 0, \qquad (\text{mod } l),$$

on a

$$\log\left[\frac{F(\zeta)}{F(1)}\right] \equiv N_1 \log\left[\frac{E_1(\zeta)}{E_1(1)}\right] + N_2 \log\left[\frac{E_2(\zeta)}{E_2(1)}\right] + \ldots + N_{\mu-1} \log\left[\frac{E_{\mu-1}(\zeta)}{E_{\mu-1}(1)}\right], \text{ mod } l.$$

c'est-à-dire en posant

$$E = E_1^{N_1} E_2^{N_2} \ldots E_{\mu-1}^{N_{\mu-1}}$$

$$\log\left[\frac{F(\zeta)E(\zeta)}{F(1)E(1)}\right] \equiv 0, \qquad (\text{mod } l),$$

ou

$$F(\zeta)E(\zeta) \equiv F(1)E(1), \qquad (\text{mod } l).$$ C. q. f. d.

§ X. — *Propriété des unités congrues, mod l^2, à un entier rationnel.*

Théorème XIII. — Si l satisfait aux trois conditions suivantes :

1° il divise un seul B_ν des $\frac{l-3}{2}$ premiers nombres de Bernoulli,

2° il ne divise pas le second facteur du nombre de classes,

3° $B_{\nu l}$ n'est pas divisible par l^3,

toute unité du corps $c\left(e^{\frac{2i\pi}{l}}\right)$ congrue, mod l^2, à un entier rationnel, est la $l^{\text{ième}}$ puissance d'une unité du corps. [Kummer[16].] (Théorème correspondant au théorème 156 pour les corps réguliers.)

Démonstration. — Soit

$$E(\zeta) = \pm \zeta^{n} \gamma_1^{N_1} \gamma_2^{N_2} \ldots \gamma_{\mu-1}^{N_{\mu-1}}$$

l'expression d'une unité quelconque $E(\zeta)$ à l'aide d'un système de $\mu - 1 = \frac{l-3}{2}$ unités fondamentales $\gamma_1, \ldots, \gamma_{\mu-1}$, et soit

$$\varepsilon(\zeta^{r^k}) = \gamma_1^{n_{k,1}} \gamma_2^{n_{k,2}} \ldots \gamma_{\mu-1}^{n_{k,\mu-1}}, \qquad (k = 0, 1, 2, \ldots, \mu-2)$$

celle des unités circulaires.

On en déduit pour $E(\zeta)$, en éliminant les γ, — ce qui est aisé en prenant les logarithmes, — l'expression

$$E(\zeta) = \pm \zeta^s \varepsilon(\zeta)^{\frac{m_0}{t}} \varepsilon(\zeta^r)^{\frac{m_1}{t}} \dots \varepsilon(\zeta^{r^{\mu-2}})^{\frac{m_{\mu-2}}{t}},$$

où nous supposons que t représente le plus petit dénominateur commun des fractions en exposant. Ce dénominateur t n'est pas divisible par l, car c'est un diviseur du déterminant des $n_{k,i}$, et ce dernier est égal au quotient $\frac{\Delta}{R}$ des déterminants des systèmes de logarithmes des unités circulaires et des unités fondamentales, c'est-à-dire (théorème 142) au second facteur du nombre de classes, facteur non divisible par l, d'après l'hypothèse.

Supposons $E(\zeta)$ congrue, mod l^2, à un entier rationnel a. Il en résulte d'abord $s=0$, car de $E(\zeta) \equiv a$, mod l^2, résulte $E(\zeta^{-1}) \equiv E(\zeta)$, mod l^2, ce qui exige, comme les unités circulaires sont réelles, $\zeta^s \equiv \zeta^{-s}$, mod l^2, et, par suite, $s=0$.

Ensuite, comme $E(1)$ est congru à a, et, par suite, à $E(\zeta)$, mod l^2, on a, en prenant les logarithmes, mod l^2 (voir § VI) :

$$\log\left[\frac{E(\zeta)}{E(1)}\right] \equiv 0, \quad (\text{mod } l^2),$$

ce qui donne, en développant d'après la seconde expression de $E(\zeta)$ et supprimant le diviseur t, non divisible par l :

$$m_0 \log\left[\frac{\varepsilon(\zeta)}{\varepsilon(1)}\right] + m_1 \log\left[\frac{\varepsilon(\zeta^r)}{\varepsilon(1)}\right] + \dots + m_{\mu-2} \log\left[\frac{\varepsilon(\zeta^{r^{\mu-2}})}{\varepsilon(1)}\right] \equiv 0, \quad (\text{mod } l^2).$$

Appliquons à $\varepsilon(\zeta^{r^k})$ la formule (8), paragraphe VI, en remarquant que toutes les dérivées d'ordre impair sont nulles pour $u=0$, parce que ces unités sont réelles, et tenant compte de ce que la norme est égale à un ; nous avons

$$(l-1)\log\left[\frac{\varepsilon(\zeta^{r^k})}{\varepsilon(1)}\right] \equiv -\log \varepsilon(1)^{l-1} + \sum_{n=1}^{n=\mu-1} r^{2nkl} \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} . X_{2n}(\zeta), \quad (\text{mod } l^2).$$

Multiplions par m_k et faisons la somme pour $k=0, 1, 2, \dots, \mu-2$, en posant pour abréger

$$M_n = \sum_{k=0}^{k=\mu-2} m_k r^{2nkl},$$

nous aurons

$$-M_0 \log \varepsilon(1)^{l-1} + \sum_{n=1}^{n=\mu-1} M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} . X_{2n}(\zeta) \equiv 0, \quad (\text{mod } l^2).$$

On trouve aisément $\varepsilon(1) = r$, et si l'on suppose, ce qui est possible, r choisi de manière que r^{l-1} soit congru à 1, mod l^2, on aura $\log \varepsilon(1)^{l-1} \equiv 0$, (mod l^2). En exprimant ensuite que les coefficients de ζ, ζ^r, etc., sont tous divisibles par l^2, on a un système de $l - 1$ congruences linéaires et homogènes indépendantes par rapport aux $\mu - 1 = \frac{l-3}{2}$ produits $M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}}$, ce qui entraîne, pour $n = 1, 2, \ldots, \mu - 1$:

$$M_n \frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} \equiv 0, \quad (\text{mod } l^2).$$

Mais on a, d'après la formule (13),

$$\frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}} = (-1)^{n-1}(r^{2nl} - 1)\frac{B_{nl}}{2nl},$$

$$\frac{d_0^{2n} \log \varepsilon(e^u)}{du^{2n}} = (-1)^{n-1}(r^{2n} - 1)\frac{B_n}{2n}.$$

D'ailleurs, on a toujours

$$\frac{d_0^{kl} \log \Phi(e^u)}{du^{kl}} \equiv \frac{d_0^{k} \log \Phi(e^u)}{du^{k}}, \quad (\text{mod } l),$$

comme on le voit en comparant les développements de $\log \left[\frac{\Phi(\zeta)}{\Phi(1)}\right]$, mod l^2, et mod l (les $X_k(\zeta)$ étant congrus dans les deux développements, d'après le théorème de Fermat). Donc $\frac{d_0^{2nl} \log \varepsilon(e^u)}{du^{2nl}}$ ne peut être divisible par l que si B_n l'est : dans le cas actuel, c'est seulement pour $n = \nu$. On a, par suite, $M_n \equiv 0$, (mod l^2), sauf pour $n = \nu$: si on suppose $\frac{B_{\nu l}}{\nu l} \equiv 0$, (mod l^2), c'est-à-dire $B_{\nu l} \equiv 0$, (mod l^3), on aura nécessairement $M_\nu \equiv 0$, (mod l). Posons alors $M_\nu \equiv \mu b l$, $M_0 \equiv \mu c$, (mod l^2), nous aurons, en multipliant M_n par r^{-2nkl} et ajoutant pour $n = 0, 1, \ldots, \mu - 1$:

$$\mu m_k \equiv \mu c + \mu b l r^{-2\nu k l}, \quad (\text{mod } l^2).$$

$$m_k = c + b l r^{-2\nu k l} + s_k l^2. \qquad (k = 0, 1, \ldots, \mu - 2)$$

En portant ces valeurs dans l'expression de $E(\zeta)$, tenant compte de ce que la norme de $\varepsilon(\zeta)$ est 1 et que, t étant premier à l, on peut déterminer deux entiers d et e tels que $td = 1 + le$, on trouve aisément

$$E(\zeta) = \left[\frac{E_1(\zeta)^{d-}}{E(\zeta)^{e}}\right]^l,$$

expression où E_1 est une autre unité, ce qui démontre le théorème.

§ XI. — *Théorème sur l'impossibilité de l'équation* (1), *dans le cas de x, y ou z divisible par l, lorsque l vérifie les trois conditions du paragraphe V.*

THÉORÈME XIV. — Si l satisfait aux trois conditions suivantes :

1° il divise un seul B_ν des $\frac{l-3}{2}$ premiers nombres de Bernoulli, et une seule fois,

2° il existe un module pour lequel E_ν n'est pas reste de $l^{\text{ième}}$ puissance,

3° $B_{\nu l}$ n'est pas divisible par l^3,

l'équation (1) est impossible en nombres entiers x, y, z premiers entre eux deux à deux, l'un d'entre eux étant divisible par une puissance quelconque de l. [Kummer[16].]

Soit z celui des trois nombres qui est divisible par l, et soit l^k la plus haute puissance de l qu'il contient, de sorte que $z = l^k z_1$. Considérons, au lieu de l'équation (1), l'équation plus générale

$$(1)' \qquad U^l + V^l = E(2 - \zeta - \zeta^{-1})^{ml} W^l,$$

U, V, W désignant des entiers premiers à l du corps $c(\zeta + \zeta^{-1})$, E une unité quelconque du corps ; $2 - \zeta - \zeta^{-1}$, c'est-à-dire $(1 - \zeta)(1 - \zeta^{-1})$, est l'un des $\frac{l-1}{2}$ facteurs égaux réels de l dans le corps $c(\zeta + \zeta^{-1})$; enfin m est supposé plus grand que un. L'équation (1) n'en est qu'un cas particulier, correspondant à

$$U = x, \quad V = y, \quad W = -z_1, \quad m = k\frac{(l-1)}{2}, \quad E = \frac{l^{kl}}{(2 - \zeta - \zeta^{-1})^{k\left(\frac{l-1}{2}\right)l}}.$$

Nous allons déduire de l'équation (1)$'$ une série d'équations de même forme :

$$U_i^l + V_i^l = E_i(2 - \zeta - \zeta^{-1})^{m_i l} W_i^l,$$

dans laquelle W_i contiendra moins de facteurs idéaux premiers que W_{i-1}. Ceci conduit à une contradiction qui entraîne l'impossibilité de l'équation (1)$'$; car W ne contenant qu'un nombre limité de facteurs premiers, on sera forcément arrêté dans la série des transformations précédentes.

Ecrivons l'équation (1)$'$

$$(U + V)(U + \zeta V) \ldots (U + \zeta^{l-1} V) = E(2 - \zeta - \zeta^{-1})^{ml} . W^l.$$

Le plus grand commun diviseur des facteurs du premier membre est $1 - \zeta$, et ce facteur $1 - \zeta$ ne peut diviser plusieurs fois que le seul facteur $U + V$, car si $U + \zeta^r V$ était divisible par $(1 - \zeta)^2$, il en serait de même, comme on le voit en changeant

ζ en ζ^{-1}, de $U + \zeta^{-r}V$, et, par suite, de $(\zeta^r - \zeta^{-r})V$, ce qui est impossible, si r n'est pas nul, V étant premier à l. On a donc, le nombre total des facteurs $1 - \zeta$ étant $2ml$,

$$\text{(A)} \qquad U + \zeta^r V = \varepsilon_r (1 - \zeta^r) I_r^l, \qquad (r = 1, 2, \ldots, l-1),$$

$$\text{(B)} \qquad U + V = \varepsilon (2 - \zeta - \zeta^{-1})^{ml - \frac{l-1}{2}} J^l,$$

les ε_r et ε étant des unités(1), les I_r des idéaux du corps $c(\zeta)$ et J un idéal du corps $c(\zeta + \zeta^{-1})$, car il ne change pas par la substitution (ζ, ζ^{-1}), vu l'équation (B).

Ces idéaux I_r et J sont des idéaux principaux.

Car on a, en éliminant U :

$$V = -\varepsilon_r . I_r^l + \varepsilon . \frac{(2 - \zeta - \zeta^{-1})^{ml - \frac{l-1}{2}}}{1 - \zeta^r} . J^l.$$

V et $\varepsilon_r I_r^l$ sont donc congrus mod l, et il en est alors de même de leurs dérivées logarithmiques (voir § 131, note)

$$\frac{d_0^{l-2\nu} \log V(e^u)}{du^{l-2\nu}} \equiv \frac{d_1^{l-2\nu} \log \varepsilon_r(e^u)}{du^{l-2\nu}} + \frac{d_0^{l-2\nu} \log I_r(e^u)^l}{du^{l-2\nu}}, \qquad (\text{mod } l);$$

mais comme $V(e^u) = V(e^{-u})$ et que $l - 2\nu$ est impair, on a

$$\frac{d_0^{l-2\nu} \log V(e^u)}{du^{l-2\nu}} \equiv 0, \qquad (\text{mod } l),$$

et de même, parce que l'on a $\varepsilon_r(\zeta) = \zeta^t \varepsilon_r(\zeta^{-1})$, d'après une propriété générale des unités (théorème 48) :

$$\frac{d_0^{l-2\nu} \log \varepsilon_r(e^u)}{du^{l-2\nu}} \equiv 0, \qquad (\text{mod } l);$$

par conséquent on a aussi

$$\frac{d_0^{l-2\nu} \log I_r(e^u)^l}{du^{l-2\nu}} \equiv 0, \qquad (\text{mod } l),$$

et il en résulte (théorème XI) que I_r est un idéal principal.

D'ailleurs, J est aussi principal d'après le corollaire du même théorème.

Le produit de $I_r(\zeta) I_r(\zeta^{-1})$ par une unité convenable est congru, mod l, à un entier rationnel.

En effet, en observant que V, ε et J ne changent pas par la substitution (ζ, ζ^{-1}), on a

$$\varepsilon_r(\zeta) I_r(\zeta)^l - \varepsilon_r(\zeta^{-1}) I_r(\zeta^{-1})^l = \frac{\varepsilon(2 - \zeta - \zeta^{-1})^{ml-\mu}(1 + \zeta^r) J^l}{1 - \zeta^r},$$

(1) Dans ce paragraphe, ε désigne une unité quelconque et non l'unité circulaire.

d'où, comme $I_r(\zeta)^l$ est congru, mod l, à un entier rationnel, et par suite à $I_r(\zeta^{-1})^l$, la congruence

$$\varepsilon_r(\zeta) \equiv \varepsilon_r(\zeta^{-1}), \qquad (\text{mod } l),$$

ce qui exige, vu la propriété générale des unités $\big(\varepsilon(\zeta) = \zeta^t \varepsilon(\zeta^{-1})\big)$,

$$\varepsilon_r(\zeta) = \varepsilon_r(\zeta^{-1}).$$

En divisant alors par $\varepsilon_r(\zeta)$ et remplaçant $2 - \zeta - \zeta^{-1}$ par $-\zeta^{-1}(1-\zeta)^2$, on a

$$(C) \qquad I_r(\zeta)^l - I_r(\zeta^{-1})^l = \varepsilon'(1-\zeta)^{(2m-1)l} J^l,$$

où ε' désigne une unité.

I_r ne figure dans toutes nos équations qu'à la puissance $l^{\text{ième}}$; on peut donc le supposer semi-primaire, c'est-à-dire congru, mod $(1-\zeta)^2$, à un entier rationnel, en le multipliant au besoin par une puissance convenable de ζ (§ 115). En décomposant alors le premier membre de (C) en ses l facteurs linéaires de la forme $I_r(\zeta) - \zeta^t I_r(\zeta^{-1})$, on voit, comme plus haut, qu'ils ont pour plus grand commun diviseur $1-\zeta$, et que le seul facteur $I_r(\zeta) - I_r(\zeta^{-1})$ est divisible plusieurs fois par $1-\zeta$ $\big($un facteur $I_r(\zeta) - \zeta^t I_r(\zeta^{-1})$ ne peut l'être si t n'est pas nul, puisque $I_r(\zeta)$ congru, mod $(1-\zeta)^2$, à une entier rationnel, est congru à $I_r(\zeta^{-1})\big)$. On a donc, les I_t' et J' étant des idéaux :

$$I_r(\zeta) - \zeta^t I_r(\zeta^{-1}) = \varepsilon_t''(\zeta) \,.\, (1-\zeta^t) \,.\, I_t'(\zeta)^l, \qquad (t = 1, 2, \ldots, l-1),$$
$$I_r(\zeta) - I_r(\zeta^{-1}) = \varepsilon''(\zeta)(1-\zeta)^{(2m-2)l+1} \,.\, J'(\zeta)^l.$$

En résolvant par rapport à $I_r(\zeta)$ et $I_r(\zeta^{-1})$, on en tire les congruences

$$\left.\begin{aligned} I_r(\zeta) &\equiv \varepsilon_t''(\zeta) I_t'(\zeta)^l, \\ I_r(\zeta^{-1}) &\equiv \varepsilon_t''(\zeta^{-1}) I_t'(\zeta^{-1})^l, \end{aligned}\right\} \quad (\text{mod } (1-\zeta)^{(2m-1)l}),$$

d'où, comme m est > 1,

$$I_r(\zeta) I_r(\zeta^{-1}) \equiv \varepsilon_t''(\zeta) \,.\, \varepsilon_t''(\zeta^{-1}) \,.\, [I_t'(\zeta) \,.\, I_t'(\zeta^{-1})]^l, \qquad (\text{mod } l),$$

$I_t'(\zeta) \,.\, I_t'(\zeta^{-1})$, idéal du corps $c(\zeta + \zeta^{-1})$, dont la $l^{\text{ième}}$ puissance est un idéal principal, est lui-même principal (corollaire du théorème XI) ; de sorte, qu'en tenant compte de la congruence ci-dessus, on a

$$\frac{d_0^{2\nu} \log [I_r(e^u) \,.\, I_r(e^{-u})]}{du^{2\nu}} \equiv \frac{d_0^{2\nu} \log [\varepsilon_t''(e^u) \,.\, \varepsilon_t''(e^{-u})]}{du^{2\nu}}, \qquad (\text{mod } l),$$

c'est-à-dire, vu la propriété générale des unités,

$$\frac{d_0^{2\nu} \log [I_r(e^u) \,.\, I_r(e^{-u})]}{du^{2\nu}} \equiv 0, \qquad (\text{mod } l),$$

ce qui prouve, vu le théorème XII, qu'en multipliant $I_r(\zeta) \,.\, I_r(\zeta^{-1})$ par une unité convenable $A_r(\zeta)$, on rend ce produit congru, mod l, à un entier rationnel. On démontrerait de plus, comme pour ε_r, que A_r est une unité du corps $c(\zeta + \zeta^{-1})$.

On déduit de $(1)'$ *une équation de même forme.*

Multiplions l'équation (A) par celle qu'on obtient par la substitution (ζ, ζ^{-1}), on a

$$U^2 + (\zeta^r + \zeta^{-r})UV + V^2 = \varepsilon_r(\zeta).\varepsilon_r(\zeta^{-1}).(2 - \zeta^r - \zeta^{-r}).[I_r(\zeta).I_r(\zeta^{-1})]^l;$$

de même,

$$U^2 + (\zeta^s + \zeta^{-s})UV + V^2 = \varepsilon_s(\zeta).\varepsilon_s(\zeta^{-1}).(2 - \zeta^s - \zeta^{-s}).[I_s(\zeta).I_s(\zeta^{-1})]^l,$$

et en élevant (B) au carré, on a

$$U^2 + 2UV + V^2 = \varepsilon(\zeta)^2.(2 - \zeta - \zeta^{-1})^{2ml-l+1}.J(\zeta)^{2l}.$$

Si on élimine $U^2 + V^2$ et UV entre ces trois équations, on a

$$\varepsilon_r(\zeta).\varepsilon_r(\zeta^{-1}).[I_r(\zeta).I_r(\zeta^{-1})]^l - \varepsilon_s(\zeta).\varepsilon_s(\zeta^{-1}).[I_s(\zeta).I_s(\zeta^{-1})]^l$$
$$= \frac{\varepsilon(\zeta)^2.(2-\zeta-\zeta^{-1})^k.(\zeta^r + \zeta^{-r} - \zeta^s - \zeta^{-s})J(\zeta)^{2l}}{(2-\zeta^r-\zeta^{-r})(2-\zeta^s-\zeta^{-s})}.$$

En posant, pour abréger,

$$A_r(\zeta).I_r(\zeta).I_r(\zeta^{-1}) = U'(\zeta), \qquad A_s(\zeta).I_s(\zeta).I_s(\zeta^{-1}) = V'(\zeta),$$
$$\frac{\varepsilon_r(\zeta).\varepsilon_r(\zeta^{-1})}{A_r(\zeta)^2} = \mathfrak{e}_r(\zeta), \qquad \frac{\varepsilon_s(\zeta).\varepsilon_s(\zeta^{-1})}{A_s(\zeta)^2} = \mathfrak{e}_s(\zeta),$$

on a

$$\mathfrak{e}_r(\zeta).U'(\zeta)^l - \mathfrak{e}_s(\zeta).V'(\zeta)^l = \frac{\varepsilon(\zeta)^2.(2-\zeta-\zeta^{-1})^k.(\zeta^r+\zeta^{-r}-\zeta^s-\zeta^{-s}).J(\zeta)^{2l}}{(2-\zeta^r-\zeta^{-p})(2-\zeta^s-\zeta^{-s})}$$

et en observant que $\zeta^r + \zeta^{-r} - \zeta^s - \zeta^{-s}$ est divisible une fois par $2 - \zeta - \zeta^{-1}$, et de même $2 - \zeta^r - \zeta^{-r}$ et $2 - \zeta^s - \zeta^{-s}$, on a, en remplaçant k par sa valeur $2ml - l + 1$, et désignant par E_1 une unité :

$$U'^l - \frac{\mathfrak{e}_s}{\mathfrak{e}_r} V'^l = E_1.(2 - \zeta - \zeta^{-1})^{(2m-1)l} J^{2l},$$

ce qui donne la congruence

$$U'^l \equiv \frac{\mathfrak{e}_s}{\mathfrak{e}_r} V'^l, \quad (\text{mod } l^2).$$

Mais U' et V' étant congrus, mod l, à des entiers rationnels, U'^l et V'^l sont congrus, mod l^2, à des entiers rationnels; donc, l'unité $\frac{\mathfrak{e}_s}{\mathfrak{e}^r}$ est congrue, mod l^2, à un entier rationnel, et elle est, d'après le théorème (XIII), la $l^{\text{ième}}$ puissance d'une unité $\mathfrak{E}(\zeta)$. En posant alors

$$U' = U_1, \quad -\mathfrak{E}V' = V_1, \quad J^2 = W_1,$$

on a l'équation

$$U_1^l + V_1^l = E_1(2 - \zeta - \zeta^{-1})^{(2m-1)l} W_1^l,$$

de même forme que celle dont on est parti et qui doit encore être vérifiée par des entiers U_1, V_1, W_1 du corps $c(\zeta + \zeta^{-1})$ premiers entre eux et à l. Par le même pro-

cédé on en déduirait une troisième et ainsi de suite indéfiniment; mais c'est impossible, car *le nombre des facteurs idéaux des* W *va en diminuant.*

En effet, on a d'abord :

$$W = I_1 I_2 \dots I_{l-1} J.$$

Comme tous les facteurs du second membre sont premiers entre eux deux à deux, W_1, qui est égal à J^2, ne pourrait donc contenir tous les facteurs idéaux de W que si tous les I étaient des unités, c'est-à-dire, d'après (A), que si $\frac{U + \zeta^r V}{1 - \zeta^r}$ était, pour toute valeur de r, une unité; en changeant alors ζ en ζ^{-1} on devrait avoir (propriété générale des unités) :

$$\frac{U + \zeta^r V}{1 - \zeta^r} = \zeta^k \frac{U + \zeta^{-r} V}{1 - \zeta^{-r}},$$

c'est-à-dire

$$U(1 + \zeta^{r+k}) + V(\zeta^r + \zeta^k) = 0.$$

Mais comme, d'après (B), on a

$$U + V \equiv 0, \quad (\text{mod } l),$$

il en résulterait

$$1 + \zeta^{r+k} - \zeta^r - \zeta^k \equiv 0, \quad (\text{mod } l),$$

c'est-à-dire

$$(1 - \zeta^r)(1 - \zeta^k) \equiv 0, \quad (\text{mod } l),$$

ce qui est impossible en dehors de l égal à 3, cas exclu, ou de k égal à 0, ce qui ne peut avoir lieu, car alors on aurait $U + V = 0$, $W = 0$.

Le théorème est ainsi complètement démontré.

D'après l'expression du premier facteur du nombre de classes pour les nombres premiers inférieurs à 100, expression donnée par Kummer (*Journal de Liouville*, tome XVI), 37, 59 et 67 sont les seuls nombres premiers non réguliers inférieurs à 100. Ils entrent une fois et une seule dans ce premier facteur. Relativement aux deux autres conditions, on a $\nu_{37} = 16$, $\nu_{59} = 22$, $\nu_{67} = 29$, et Kummer a trouvé Ind $E_{16} \equiv 24$, mod 37, pour le facteur idéal de 149 correspondant à $\zeta - 17$, Ind $E_{22} \equiv 50$, mod 59, pour l'idéal de 709 correspondant à $\zeta - 385$, Ind $E_{29} \equiv 4$, mod 67, pour l'idéal de 269 correspondant à $\zeta - 47$ (2 étant choisi dans les trois cas pour la racine primitive, mod l, qui figure dans E_ν). Enfin, les nombres $B_{\nu l}$ sont congrus respectivement à 35×37^2, mod 37^3, 41×59^2, mod 59^3, et 49×67^2, mod. 67^3. Les trois conditions requises pour la démonstration sont donc remplies, de sorte que l'impossibilité de l'équation (1) est établie pour tous les exposants premiers l inférieurs à 100.

En dehors du résultat de Kummer, il a été obtenu peu de résultats nouveaux, dans le cas où xyz est $\equiv 0$, (mod l).

Signalons seulement un résultat négatif, qui conduit à abandonner une méthode qui paraissait s'appliquer aussi bien aux deux cas de $xyz \equiv 0$ ou $\not\equiv 0$, (mod l).

Il paraissait naturel de chercher si la congruence $x^n + y^n + z^n \equiv 0$, mod p, ne serait pas impossible en nombres entiers premiers à p, pourvu seulement qu'on prît le module p suffisamment grand : car, dans le cas de l'affirmative, l'impossibilité de l'équation (1) se trouverait complètement démontrée. Mais Dickson a montré que cette méthode devait être abandonnée, car :

Théorème XV. — La congruence $x^n + y^n + y^n \equiv 0$, mod p, a toujours des solutions x, y, z, premières à p, dès que p dépasse une certaine limite. (Dickson, *On the congruence* $x^n + y^n + z^n \equiv 0$, mod p; et *Lower limit for the number of sets of solutions of* $x^e + y^e + z^e \equiv 0$, mod p. J. f. d. Mathematik, Band 135.)

Hurwitz a donné de cette proposition une démonstration plus élémentaire tout en la généralisant. (*Ueber die Congruenz* $ax^e + by^e + cz^e \equiv 0$, mod p. J. f. d. Mathematik, Band 136.)



ERRATA ET RECTIFICATIONS

Page 9, ligne 12. *Au lieu de* au domaine, *lire :* ou domaine.

10, 13. *Au lieu de* α_m, *lire :* α^m.

» 15. Dans l'énoncé du théorème 2, l'expression *fonction entière* est synonyme de *polynôme entier* (et non de *série* entière); il en est de même dans tout l'ouvrage.

» 15 et 21. *Après* coefficients entiers, *ajouter :* rationnels.

12. *Remplacer la* ligne 18 *par :*

$$r_s = \frac{|1, \alpha, \dots, \omega, \quad \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|} = \frac{|1, \alpha, \dots, \omega, \dots, \alpha^{m-1}| \times |1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|}{|1, \alpha, \dots, \alpha^{s-1}, \dots, \alpha^{m-1}|^2} = \frac{A_s}{d(\alpha)}.$$

Page 12. Dans l'avant-dernière ligne, *remplacer* $O_2^{(2)}, \dots, O_s^{(2)}$ *par :* $O_2^{(1)}, \dots, O_s^{(1)}$.

13, ligne 5. *Après* nombre, *ajouter :* entier.

14. *Intervertir la* ligne 19 *et la* ligne de points *suivante*.

15, ligne 1. *Ajouter à la fin :* ou module $\mathfrak{a}$.

» 3. *Au lieu de* d'après, *lire :* suivant.

» 10. *Après* coefficients, *ajouter :* entiers.

» 22. *Après* restes, *ajouter :* positifs.

». Dans l'antépénultième ligne, *après* premiers, *ajouter :* entre eux.

16, ligne 15. *Au lieu de* entier ω, *lire :* entier algébrique ω.

» 25. *Au lieu de* puissance, *lire :* forme.

» 28. *Remplacer le* point-virgule après *n par une* virgule.

17, 3. *Après* (α), *ajouter un* point-virgule.

» 23. *Ajouter un* point-virgule *avant :* par hypothèse.

19, 1. *Au lieu de* claire, *lire :* clair.

» 14. *Au lieu de* puissances de a, *lire :* puissances de u.

» 17. *Au lieu de b, lire :* G.

» 29. *Au lieu de* égal, *lire :* équivalent.

» 31. *Après* première, *ajouter :* P.

Page 20. Dans l'énoncé du théorème 17, *après* nombre, *ajouter :* premier.

21, ligne 22. *Au lieu de* incongrus à, *lire :* incongrus suivant.

» Dans l'antépénultième ligne, *remplacer* les formes *par :* des formes.

22, ligne 2. *Au lieu de* exciterait, *lire :* existerait.

23, 17. *Au lieu de* premier, *lire :* premiers.

24, 8. *Au lieu de* d'après, *lire :* suivant.

» 11. *Remplacer les coefficients* α, α_1, etc., *par :* a, a_1, etc.

» 14. *Au lieu de* Fx, *lire :* F(x).

25, 8 et 9. *Au lieu de* d'après, *lire :* suivant.

» 12. *Mettre des* virgules *après* alors, *et après* suivant $\mathfrak{p}$.

» 13. *Au lieu de* ($\mathfrak{p}$), *lire* ($\mathfrak{p}^2$).

» 14. *Au lieu de* α_i, *lire :* α_l.

» 16. *Au lieu de* α_e, *lire :* α_l.

» Dans l'antépénultième ligne, *mettre une* virgule *entre* ρ *et* P(ρ).

26, ligne 6. *Mettre :* $d =$, *devant le carré du déterminant.*

27. Dans la dernière ligne, *après* et, *ajouter :* est.

28. *Ajouter à la fin :*

« Toutefois, si (p) n'est divisible que par $\mathfrak{p}$ et non par $\mathfrak{p}^2$, ces coefficients peuvent être tous divisibles par $\mathfrak{p}^2$. S'il en est ainsi, il suffit, pour obtenir une fonction Π_1 satisfaisant aux conditions de l'énoncé, de prendre $\Pi_1 = \Pi(x; u_1, \ldots, u_m) + kp$, k étant un entier quelconque premier à p ». (G. H. et T. G.)

29, ligne 6. *Au lieu de* suites, *lire :* seules.

» 12. *Au lieu de* $\mathfrak{p}^2$, *lire :* $\mathfrak{p}^e$.

» 13. *Au lieu de* où $e' < e$ et F, *lire :* où l'on a $e' < e$ et où F est.

» Dans l'antépénultième ligne, *remplacer* nombre *par :* membre.

30, ligne 16. *Au lieu de* précédentes, *lire :* précédents.

31, 1. *Au lieu de* des U_{ik}, *lire :* les U_{ik}.

32, 15. *Supprimer les* points *après :* $\Pi^{e'}$.

» 6, à partir du bas. *Au lieu de* nombre, *lire :* membre.

34, 7. *Au lieu de* choisis, *lire :* choisi.

36, 1. *Au lieu de* de, *lire :* le.

37, 7, à partir du bas. *Après* degré, *ajouter :* r.

» 4, à partir du bas. *Au lieu de* M, *lire :* m.

38, 7. *Remplacer le troisième terme écrit par :* $(\Xi^{(r-1)})^{r-1}$.

» 15. *Remplacer* Ω_1 *par :* Ω'_1.

» 22. *Au lieu de* déterminantes, *lire :* déterminants.

» Dans la dernière ligne, *au lieu de* déterminant, *lire :* discriminant.

40, ligne 5. *Après* et, *ajouter :* de.

41, 4. *Au lieu de* conjuguées, *lire :* conjugués.

Page 41, ligne 19. *Remplacer* $f_{s'}$ *par :* f_s.

» 20. *Rectifier la seconde égalité* (8) *de la façon suivante :*

$$f_{s'} = \frac{1}{i\sqrt{2}}\left[(\omega_1^{(s)} - \omega_1^{(s')})u_1 + \ldots + (\omega_m^{(s)} - \omega_m^{(s')})u_m\right].$$

43, 6, à partir du bas. *Après* formons, *ajouter :* au moyen de ces nombres.

46, 6. *Remplacer* $\Lambda^{\frac{1}{2}\lambda_r t}$ *par :* $\Lambda_r = e^{\frac{1}{2}\lambda_r t}$.

47, 7. Dans le dernier crochet, *remplacer* $l_1(\alpha)$ *par :* $l_r(\alpha)$.

49, 1 et 2. *Remplacer* deux quelconques de ces puissances *par :* il y aura deux de ces puissances qui.

» 6. *Supprimer :* chaque fois.

» 7. *Au lieu de* H^T, *lire :* H_T.

» 8. *Au lieu de* $M_I^{M_T}$, *lire :* $H_T^{M_T}$.

» 9. *Au lieu de* composants, *lire :* exposants de.

» Dans l'avant-dernière ligne, *au lieu de* ρ^H, *lire :* ρ^M.

52, ligne 10, à partir du bas. *Au lieu de* (j), *lire :* n(j).

53, 5, à partir du bas. *Au lieu de* déterminantes, *lire :* déterminants.

54, 4. *Au lieu de* déterminants, *lire :* déterminant.

55, 8. *Mettre une* virgule *après* et, *et remplacer le* point-virgule *après* $= 0$ *par une* virgule.

» 10. *Au lieu de* $|\xi^{(1)}(\xi_1)$, *lire :* $|\xi^{(1)}(\xi)|$.

57, 6. *Remplacer* $l_{r-1}(\eta)$ *par :* $l_{r+1}(\eta)$.

» 8. *Remplacer* $l_{r+1}(\eta) = l_{r+1}(\xi)$ *par :* $l_{r+2}(\eta) = l_{r+2}(\xi)$.

58, 17. *Après* norme, *ajouter :* n.

60, 8. *Après* nombres premiers, *ajouter :* p.

» 9. *Supprimer :* du corps.

» 17. *Au lieu de* h_{q-1}, *lire :* $h_q - 1$, *et au lieu de* $A_q^{h_q}$, *lire :* $A_1^{h_1}$.

» 9, à partir du bas. *Au lieu de* puissance de H_s, *lire :* puissance de H_1.

61. Dernière ligne, *remplacer la dernière égalité par :* $\chi_q(A) = e^{\frac{2i\pi r_q}{h_q}}$.

62, ligne 4, à partir du bas. *Après* entiers, *ajouter :* des coefficients.

63. Au bas de la page, *supprimer les* accents *des* α *dans la première ligne du déterminant.*

64. *L'anneau* est ce que Dedekind a appelé *ordre*.

» ligne 5, à partir du bas. *Après* discriminant, *supprimer :* de.

66, 3. *Au lieu de* $\mathfrak{z} = \mathfrak{f}\theta$, *lire :* $\mathfrak{z} = \mathfrak{f}\mathfrak{d}$.

» 2, à partir du bas. *Au lieu de* déterminant, *lire :* discriminant.

71. Dans la formule au bas de la page, *faire passer* $w R_r$ *au dénominateur, et* $w_r R$ *au numérateur.*

73. *Au lieu de* corps des nombres de Galois, *lire :* corps de nombres de Galois.

Page 92, ligne 3. *Au lieu de* engendrent des classes, *lire :* engendrent les classes.

108, 13. *Après* est congru, *ajouter :* mod w.

» 14. *Au lieu de* dans $k(\sqrt{m})$ un nombre entier, *lire :* un nombre entier dans $k(\sqrt{m})$.

138, 17. *Au lieu de* Si le corps K, *lire :* Le corps K qui.

146, 1 et 4. *Au lieu de* différent, *lire :* différant.

160, 15, à partir du bas. *Au lieu de* mod $(\mathbf{j})$, *lire :* mod $\mathbf{j}$.

161, 2. *Au lieu de* $(\zeta\lambda - 1)^u$, *lire :* $(\xi\lambda - 1)^u$.

180, 4, à partir du bas. *Au lieu de* $\prod_{(e)}(1 - e)$, *lire :* $\prod_{(e)}(1 - s^e)$.

185. A la dernière ligne, *au lieu de* note I, *lire :* note V.

199, ligne 2, à partir du bas. *Lire a la fin :* $\zeta\mathbf{M}$, *au lieu de :* $\mathbf{M}$.

203, 16 et 18. *Au lieu de* S^{-1}, *lire :* S^{l-1}.

» 25. *Au lieu de* différent, *lire :* différant.

208, 19, à partir du bas. *Au lieu de* $\mu(1 - \lambda^{k-1})^l \equiv 1 - \lambda^{lu}$, *lire :* $\mu(1 - \lambda^{k-1})^{lu} \equiv 1 - \lambda^l$.

222, 11, à partir du haut et ligne 2 à partir du bas. *Au lieu de* x, *lire :* $\varkappa$.

223, 12, à partir du bas. *Au lieu de* 1_1, *lire :* 1.

263, 5. *Au lieu de* paragraphes, *lire :* paragraphe.

323, 3, à partir du bas. *Au lieu de* et que, *lire :* et.

INDEX ALPHABÉTIQUE DES DÉFINITIONS

TABLE DES MATIÈRES

Chapitre VI. — *Unités du corps.*

Chapitre VII. — *Classes d'idéaux.*

Chapitre VIII. — *Les formes décomposables du corps.*

Chapitre IX. — *Les anneaux du corps.*

DEUXIÈME PARTIE. — **Corps de Galois.**

Chapitre X. — *Idéaux premiers du corps de Galois et de ses sous-corps.*

Chapitre XI. — *Différents et discriminants du corps de Galois.*

Chapitre XII. — *Rapports entre les propriétés arithmétiques et algébriques d'un corps de Galois.*

Chapitre XIII. — *Composition des corps.*

Chapitre XIV. — *Idéaux premiers du premier degré. Notion de classe.*

Chapitre XV. — *Corps cyclique relatif de degré premier.*

TROISIÈME PARTIE. — Les corps quadratiques.

Chapitre XVI. — *Décomposition des nombres dans un corps quadratique.*

Chapitre XVII. — *Genres dans un corps quadratique et leurs caractères.*

QUATRIÈME PARTIE. — **Les corps circulaires.**

Chapitre XXXII. — *Classes d'idéaux invariantes et genres d'un corps kummerien régulier.*

Chapitre XXXIII. — *Loi de réciprocité des résidus de $l^{\text{ièmes}}$ puissances dans un corps circulaire régulier.*

Chapitre XXXIV. — *Nombre des genres d'un corps kummerien régulier.*

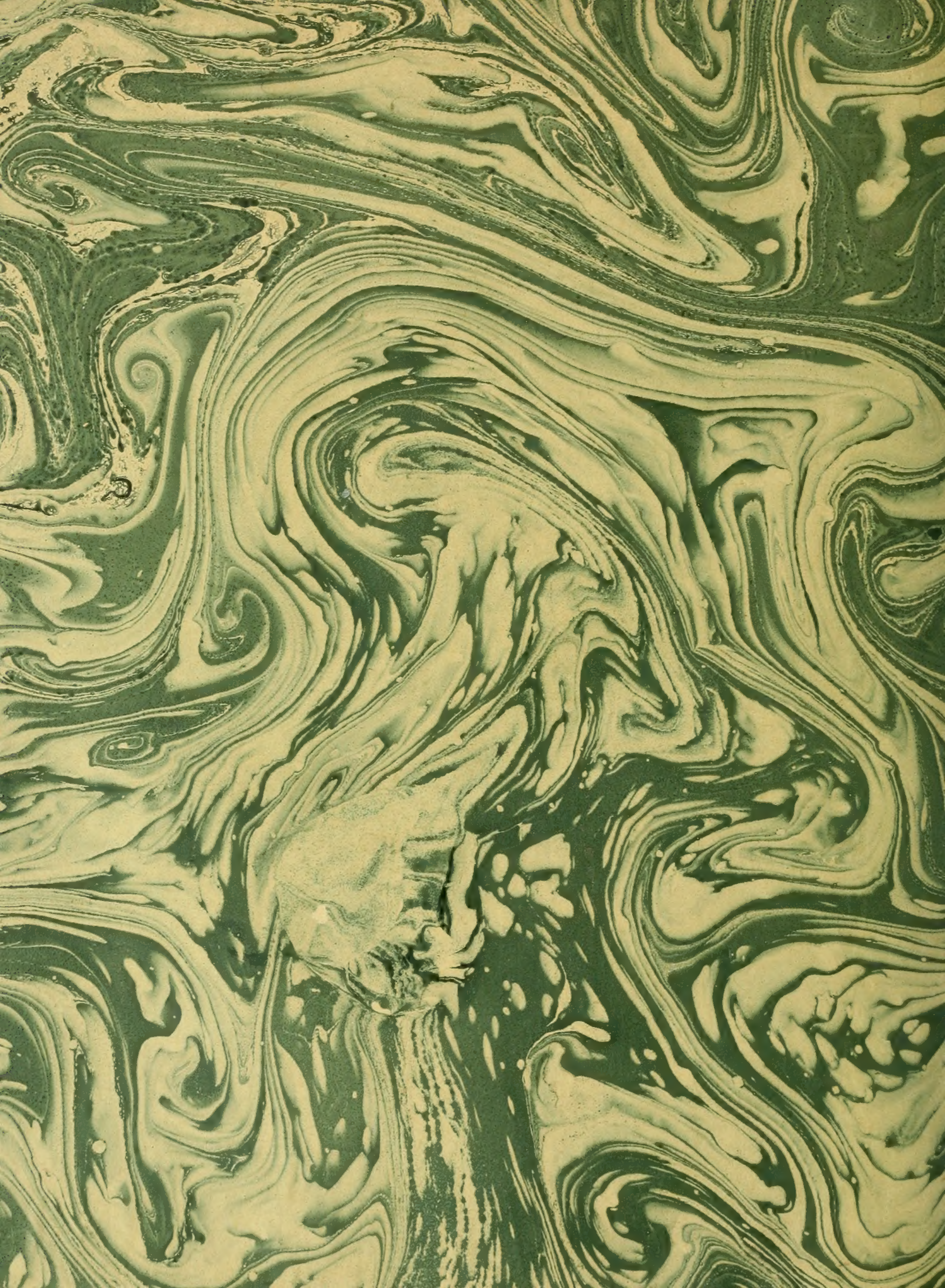
Chapitre XXXV. — *Nouvelle méthode pour la théorie d'un corps kummerien régulier.*

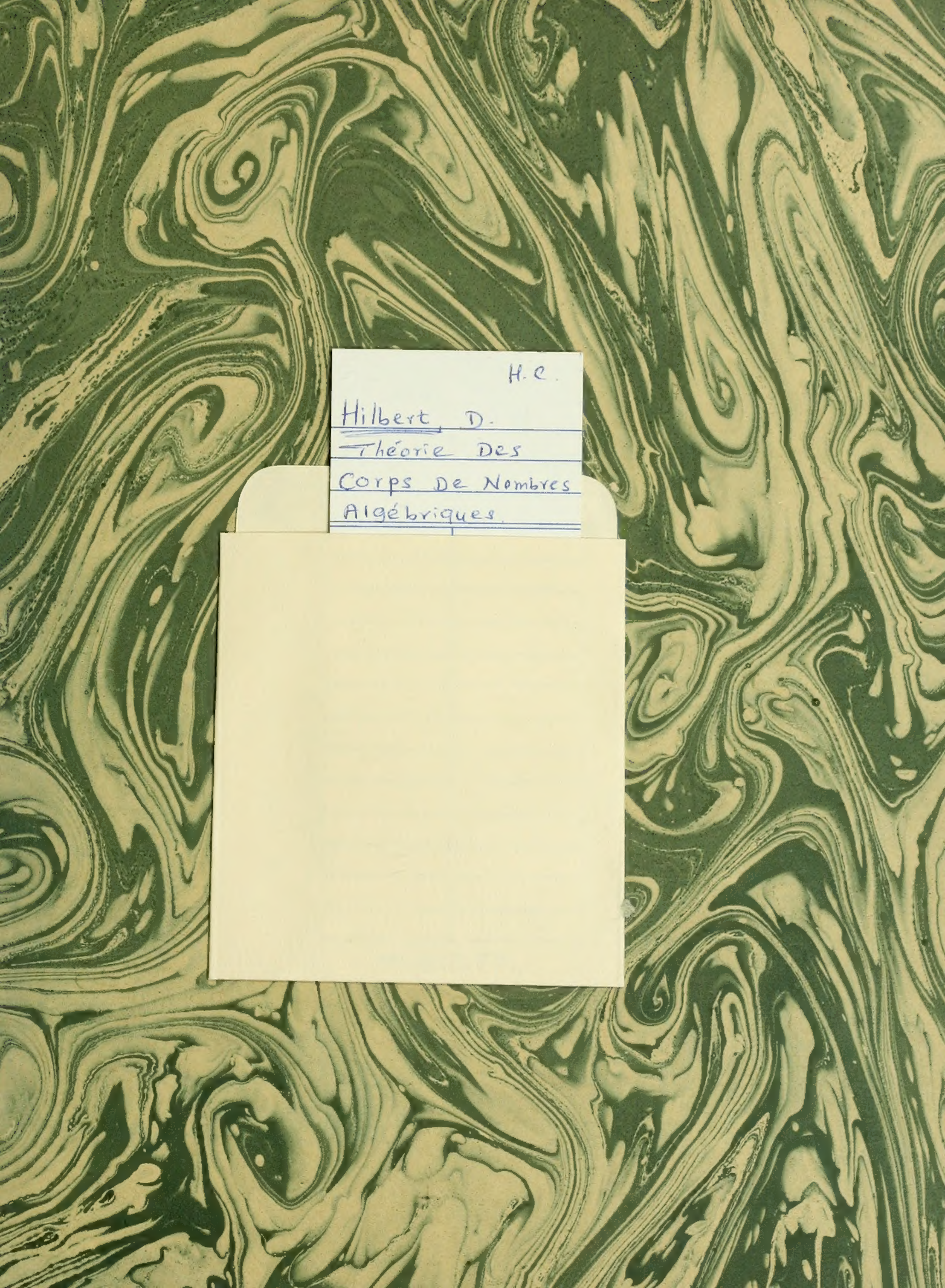
NOTES DE M. G. HUMBERT

NOTES DE M. TH. GOT

Toulouse. — Imprimerie Douladoure-Privat, rue Saint-Rome, 39. — 9994

LAVAL. — IMPRIMERIE L. BARNÉOUD ET Cie.




H. C.
Hilbert, D.
Théorie Des
Corps De Nombres
Algébriques.

